UNIVERSITY
OF MICHIGAN

JUL 9 1952

MATHEMATICS
LIBRARY

CANADIAN JOURNAL OF MATHEMATICS

Journal Canadien de Mathématiques

VOL. IV - NO. 3
1952

Isoperimetric problems in the calculus of variations — William Karush — 257

The index of an extremal arc — William Karush — 281

Cyclic affine planes — A. J. Hoffman — 295

Finite projective geometries — Gerald Berman — 302

The factors of graphs — W. T. Tutte — 314

Some characterizations of generalized manifolds with boundaries — Paul A. White — 329

On the number of solutions of some general types of equations in a finite field — Olin B. Faircloth — 343

Abelian quadratic forms — K. G. Ramanathan — 352

Groups with a certain condition on conjugates — Franklin Haimo — 369

On a conjecture by J. H. Chung — G. de B. Robinson — 373

On the irreducible representations of the symmetric group — Masaru Osima — 381

Published for
THE CANADIAN MATHEMATICAL CONGRESS
by the
University of Toronto Press

EDITORIAL BOARD

H. S. M. Coxeter, A. Gauthier, R. D. James, R. L. Jeffery, G. de B. Robinson, H. Zassenhaus

with the co-operation of

A. S. Besicovitch, R. Brauer, D. B. DeLury, P. A. M. Dirac, R. Godement, I. Halperin, L. Infeld, S. MacLane, G. Pall, L. Schwartz, J. L. Synge, W. J. Webber

The chief languages of the *Journal* are English and French.

Manuscripts for publication in the *Journal* should be sent to the *Editor-in-Chief*, H. S. M. Coxeter, University of Toronto. Everything possible should be done to lighten the task of the reader and the notation and reference system should be carefully thought out. Every paper should contain an introduction summarizing the results as far as possible in such a way as to be understood by the non-expert.

All other correspondence should be addressed to the *Managing Editor*, G. de B. Robinson, University of Toronto.

The *Journal* is published quarterly. Subscriptions should be sent to the *Managing Editor*. The price per volume of four numbers is $6.00. This is reduced to $3.00 for individual members of the following Societies:

Canadian Mathematical Congress
American Mathematical Society
Mathematical Association of America
London Mathematical Society
Société Mathématique de France

The Canadian Mathematical Congress gratefully acknowledges the assistance of the following towards the cost of publishing this Journal:

University of British Columbia	Carleton College
Ecole Polytechnique	Université Laval
Loyola College	University of Manitoba
McGill University	McMaster University
Université de Montréal	Queen's University
Royal Military College	University of Toronto

National Research Council of Canada
and the
American Mathematical Society

AUTHORIZED AS SECOND CLASS MAIL, POST OFFICE DEPARTMENT, OTTAWA

L

S

2

I

ISOPERIMETRIC PROBLEMS IN THE CALCULUS OF VARIATIONS

WILLIAM KARUSH

1. Introduction. We are concerned with establishing sufficiency theorems for minima of simple integrals of the parametric type in a class of curves with variable end points and satisfying isoperimetric side conditions. The results which are obtained involve no explicit assumptions of normality. Such results can be derived by transforming our problem to a problem of Bolza and using the latest developments in the theory of that problem. More recently [6] an indirect method of proof has been published. Our object is to present a direct method of proof without transformation of the problem which is based upon a generalization of the classical theory of fields.

We treat first the case of no isoperimetric side conditions. The main theorem to be proved for this problem is Theorem 2.2, appearing at the end of §2. The proof is based upon a theory of fields which is an extension of the theory of fields for fixed end points, and was suggested by a similar treatment for a problem in non-parametric form [5].

The isoperimetric problem is formulated in §6, where the main result of the paper, Theorem 6.1, is stated. The proof of this theorem makes use of a family of broken extremals whose properties are described in §7. The results of §7 are extensions of those of Birkhoff and Hestenes [1]. The proof of Theorem 6.1 is completed first for the so-called strongly normal case; in §9 it is shown how the normality assumption may be lifted [cf. 2].The final §10 is devoted to several corollaries of Theorem 6.1.

2. The non-isoperimetric problem. In the present section we formulate precisely the non-isoperimetric problem of the calculus of variations and we shall study first, and state, some standard definitions and properties.[1]

The function to be minimized will be taken to have the form

$$I(C) = g(a) + \int_{t_1}^{t_2} f(a, y, y')dt, \tag{2.1}$$

and is defined over a class of admissible parametric arcs C of the form

$$a_h, y_i(t) \qquad (h = 1,2,\ldots,r;\ i = 1,2,\ldots,n;\ t_1 \leqslant t \leqslant t_2) \tag{2.2}$$

in ay-space, satisfying a set of end conditions

$$y_i(t_s) = y_{is}(a) \qquad (s = 1,2). \tag{2.3}$$

Received August 29, 1950.

[1]Throughout this paper we shall use many of the standard results found in reference [3].

It is understood that the a_h are constants independent of t. We denote the derivative of $y_i(t)$ by $y'_i(t)$. The functions g, f, y_{ti} are assumed to be of class C^4 in a region $\mathfrak{R}$ of points (a, y, y'), and f is taken to be positively homogeneous of degree one. This region is assumed to have the property that if the element (a, y, y') is in $\mathfrak{R}$ then[2] $y'_i f_{y'_i y'_j} \neq 0$ and (a, y, ky') is in $\mathfrak{R}$ for $k > 0$. An element in $\mathfrak{R}$ is called *admissible*. By an *admissible arc* is meant a continuous arc having a representation[3] (2.2) with the following properties:

(1) $t_1 t_2$ can be partitioned into a finite number of (closed) sub-intervals on each of which the functions $y_i(t)$ are of class C';

(2) each element (a, y, y') of the arc is admissible.

An admissible element is *non-singular* in case the matrix

$$||f_{y'_i y'_j}||$$

has rank $n - 1$ at that element (from the homogeneity of f, this is the maximum rank). Equivalently, an element is non-singular in case the determinant

$$\begin{vmatrix} f_{y'_i y'_j} & y'_i \\ y'_j & 0 \end{vmatrix}$$

does not vanish.

An *extremal* E is an admissible arc (2.2) of class C'' which satisfies the Euler equations

$$f_{y_i} - \frac{d}{dt} f_{y'_i} = 0. \tag{2.4}$$

Such an arc is a *non-singular extremal* in case each of its elements $(a, y(t), y'(t))$ is non-singular. It is well known [3, p. 108] that when a non-singular extremal is represented with arc length as parameter, then the functions (2.2) have the same class as f, namely C^4, in the present case.

From standard existence theorems on differential equation one obtains the following result [3].

THEOREM 2.1. *Every non-singular extremal E is a member of an $(r + 2n)$-parameter family of extremals*

$$a_h, \quad y_i(t,a,b,c) \qquad (h = 1,2,\ldots,r;\ i = 1,2,\ldots,n) \tag{2.5}$$

for special values $a_h = a_{h0}, b_i = b_{i0}, c_i = c_{i0}, t_1 \leqslant t \leqslant t_2$. The functions y_i, y'_i are defined and of class C'' in a neighbourhood of the values (t, a, b, c) belonging to E, and satisfy the equation

$$\nu' Q''_i = 0. \tag{2.6}$$

The determinant

$$\begin{vmatrix} y_{t b_j} & y_{t c_j} \\ y'_{t b_j} & y'_{t c_j} \end{vmatrix} \tag{2.7}$$

[2] Here and elsewhere a repeated index indicates summation over that index.

[3] For brevity we often refer to the representation (2.2) as the arc itself.

is different from zero along E. The parameters b_i, c_i may be taken to be the values of y_i, y'_i at a fixed value $t = t_0$ on the interval $t_1 t_2$. Furthermore, there exists a neighbourhood $\mathfrak{F}$ of E in ay-space such that an extremal in $\mathfrak{F}$ with end values (a, y_1) and (a, y_2) sufficiently close to the end values of E is an extremal of the family (2.5).

Although the parameters b, c appearing above are not independent we prefer to leave them in the present form.

An extremal E satisfies the *transversality condition* if, along E, the equation

$$dg + [f_{y'_i} dy_{ti}]_1^2 + \int_{t_1}^{t_2} f_{a_h} da_h dt = 0 \tag{2.8}$$

is an identity in da_h. The expression in brackets denotes

$$f_{y'_i}(a,y(t_2),y'(t_2))dy_{t2} - f_{y'_i}(a,y,(t_1),y'(t_1))dy_{t1},$$

where summation over the repeated index i is understood as remarked earlier.

The extremal E satisfies the *Weierstrass condition* Π_N if, for every element (a, y, y') in a neighbourhood N of those on E,

$$E(a,y,y',Y') \geqslant 0 \tag{2.9}$$

for every $(Y') \neq (ky')$, $k > 0$, such that $a, y, Y')$ is admissible. Here the function E is defined by

$$E = f(a,y,Y') - Y'_i f_{y'_i}(a,y,y').$$

Using the homogeneity of f, this function may be expressed in other forms. One consequence of the homogeneity is that $E = 0$ whenever $(Y') = (ky')$, $k > 0$.

The extremal E satisfies the *Clebsch condition* if, along E,

$$f_{y'_i y'_j} \sigma_i \sigma_j \geqslant 0$$

for all $(\sigma) \neq (ky')$, k arbitrary. The equality holds automatically for $(\sigma) = (ky')$, k arbitrary.

The second variation of I along an extremal E will be taken to be

$$I_2(a,\eta) = b_{hk} a_h a_k + \int_{t_1}^{t_2} 2\omega(t,a,\eta,\eta')dt \tag{2.10}$$

where

$$b_{hk} = g_{hk} + [f_{y'_i} y_{tihk}]_1^2, \tag{2.11a}$$

$$2\omega = f_{y_i y_j}\eta_i\eta_j + 2f_{y_i y'_j}\eta_i\eta'_j + f_{y'_i y'_j}\eta'_i\eta'_j + 2f_{y_i a_h}\eta_i a_h + 2f_{y'_i a_h}\eta'_i a_k + f_{a_h a_k} a_h a_k. \tag{2.11b}$$

In the derivatives of f, g, and y_{ti} we understand that the arguments belong to E. Subscripts h, k on the latter two functions indicate differentiation with respect to a_h, a_k. The constants a_h and the functions $\eta_i(t)$ are required to satisfy continuity conditions like those for admissible arcs. The non-parametric arcs thereby defined in $at\eta$-space are called *admissible variations*. An admissible variation of the form $(0,\eta)$ with $\eta_i(t) = w(t)y'_i(t)$ is a *tangential variation*.

The second variation I_2 will be said to be *positive* along E if $I_2(a,\eta) > 0$ for every non-tangential variation which satisfies along E the end conditions

$$\eta_i(t_s) = y_{isk}a_k \qquad (s = 1,2). \tag{2.12}$$

From the homogeneity of f it may be proved that for a tangential variation satisfying (2.12), i.e., vanishing at the end points, the equality $I_2 = 0$ holds.

An *accessory extremal* is an admissible variation of class C'' for which

$$\omega_{\eta i} - \frac{d}{dt}\,\omega_{\eta' i} = 0. \tag{2.13}$$

The accessory extremal is *special* [4] in case $y'_i\eta'_i = \text{constant}$, i.e.,

$$y'_i\eta''_i + y''_i\eta'_i = 0. \tag{2.14}$$

It may be shown that if $w(t)$ is an arbitrary function of class C' then the variation $(0, wy')$ is a solution of (2.13).

Let P_3P_4 be points on the extremal E defined by parametric values $t_3 \neq t_4$. We say that P_4 is *conjugate* to P_3 if there exists a special accessory extremal of the form $(0,\eta)$ which vanishes at t_3 and t_4 but is not identically zero between these values.

Two special accessory extremals $(0,\eta)$ and $0,u)$ are *conjugate* in case

$$\eta_i\omega_{\eta' i}(0,u,u') = u_i\omega_{\eta' i}(0,\eta,\eta'). \tag{2.15}$$

A set of special accessory extremals form a *conjugate system* in case every pair of the set is conjugate. Two such extremals are conjugate if and only if (2.15) holds at one point of the interval; this is a consequence of the well-known fact that the two members of the equation always differ by a constant for special accessory extremals.

Our first objective is to establish the following sufficiency theorem.

THEOREM 2.2 *If a non-singular extremal E which does not intersect itself satisfies the end conditions* (2.3), *the transversality condition* (2.8), *the Weierstrass condition* Π_N, *and is such that the second variation of I along E is positive, then there exists a neighbourhood $\mathfrak{F}$ of E in ay-space such that $I(C) > I(E)$ for every admissible arc C in $\mathfrak{F}$ satisfying* (2.3) *and not identical with E.*

3. Mayer fields. We present in this section a theory of fields which is a generalization of the theory of fields for the fixed end point case. Our results here will assume that a given extremal E is already imbedded in a field; in the next section we shall show how this imbedding may be carried out.

By a *Mayer field* we shall mean a region $\mathfrak{F}$ in ay-space and a set of slope functions $p_i(a, y)$ $(i = 1, 2, \ldots, n)$ of class C'' on $\mathfrak{F}$ with the following properties. For every (a, y) in $\mathfrak{F}$ the element $(a, y, p\ (a, y))$ is admissible, and the Hilbert integral

$$I^*(C) = g(a) + \int_{t_1}^{t_2} y'_i f_{y' i}(a,y,p)dt \tag{3.1}$$

is independent of the path in $\mathfrak{F}$ in the sense that I^* has the same value for any

two admissible arcs in $\mathfrak{F}$ with the same end points (a, y_1) and (a, y_2). Notice that if $\mathfrak{F}$ forms a field with $p_i(a, y)$ then this region forms a field with $k(a, y)p_i(a, y)$ for an arbitrary function $k(a, y) > 0$ of class C''.

For an admissible arc C in $\mathfrak{F}$,

$$I(C) - I^*(C) = \int_{t_1}^{t_2} E(a,y,p,y')dt. \tag{3.2}$$

An arc which has a representation (2.2) that satisfies $y'_i = p_i(a, y)$ will be called *an extremal of the field*. The following results are standard. An extremal of a field is an extremal in the sense of satisfying the Euler equations; through each element (a, y) there passes one and only one extremal of a field; for an extremal of a field, $I^*(E) = I(E)$.

THEOREM 3.1. *Let E be an extremal of a field $\mathfrak{F}$ which satisfies the end conditions* (2.3). *Suppose that for each (a, y) in $\mathfrak{F}$,*

$$E(a,y,p(a,y),y') > 0$$

whenever (a, y, y') is admissible and $(y') \neq (kp)$, $k > 0$. Suppose also that $I^*(C) \geq I^*(E)$ for every admissible C in $\mathfrak{F}$ satisfying (2.3), *the equality holding if and only if C and E have the same components a_h. Then $I(C) > I(E)$ for every admissible C in $\mathfrak{F}$ satisfying* (2.3) *and not identical with E.*

For, from (3.2), $I(C) \geq I^*(C) \geq I^*(E) = I(E)$ for C as in the theorem. Suppose $I(C) = I(E)$. Then the right side of (3.2) is zero, and from the assumption on E it follows that $y'_i(t) = k(t)p_i(a, y)$ with $k(t) > 0$. Introducing the parameter

$$\tau = \int_{t_1}^{t} k(t)dt,$$

one readily verifies that C is an extremal of the field. From $I^*(C) = I^*(E)$ it follows by assumption that C and E have the same components (a) and hence the same end points. Since a unique extremal of a field passes through a point we conclude that C and E are identical.

The last theorem suggests the problem of minimizing I^*. Our next theorem deals with that problem. But first we compute the second variation $I_2^*(a, \eta)$ of I^* along E. It is

$$I_2^*(a,\eta) = b_{hk}a_ha_k + 2\int_{t_1}^{t_2} [\omega + (\eta'_i - \pi_i)\omega_{\eta'_i}]dt, \tag{3.3}$$

where

$$\pi_i(t,a,\eta) = p_{iy_h}a_h + p_{iy_j}\eta_j,$$

and the remaining symbols are defined by (2.11); the arguments in ω and its derivatives are (t, a, η, π).

THEOREM 3.2. *Let E be an extremal of a field which satisfies the transversality conditions* (2.8) *and end conditions* (2.3). *Suppose $I_2^*(a, \eta) > 0$ for every admissible*

variation with $(a) \neq (0)$ *which satisfies the end conditions* (2.12). *Then there exists a neighbourhood* $\mathfrak{F}$ *of* E *in ay-space such that for every admissible* C *in* $\mathfrak{F}$ *satisfying* (2.3) *we have* $I^*(C) > I^*(E)$, *the equality holding if and only if* C *and* E *have the same components* a_k.

For the proof we may assume that $a_k = 0$ for E. Let $a_{kk}, \eta_{ik}(t) (k = 1, 2, \ldots, r)$ be r admissible variations of class C'' satisfying (2.12), $a_{kk} = \delta_{kk}$ (Kronecker delta). Let

$$Y_i(t, a) = y_i(t) + \eta_{ik} a_k,$$

$$h_{is}(a) = \frac{y_{is}(a) - Y_i(t_s, a)}{t_2 - t_1} \qquad (s = 1,2),$$

where $y_i(t)$ belongs to E. Define an r-parameter family of admissible arcs:

$$a_k y_i(t,a) = Y_i(t,a) + h_{i1}(a)(t_2 - t) + h_{i2}(a)(t - t_1). \tag{3.4}$$

This family satisfies (2.3) and contains E for $(a) = (0)$. Let $I^*(a)$ be the value of I^* along (3.4). By direct calculation and the Euler equations (2.4) we find that at $a = 0$,

$$dI^* = dg + [f_{y'_i} dy_{is}]_1^2 + \int_{t_1}^{t_2} f_{a_k} da_k dt,$$

$$d^2 I^* = I_2^*(a, \eta),$$

where $a_k = da_k$, $\eta_i = \eta_{ik} da_k$. Hence $dI^* = 0$, $d^2 I^* > 0$ for $(da) \neq (0)$, and $I^*(a)$ has a proper relative minimum at $(a) = (0)$. Therefore $I^*(a) > I^*(0) = I^*(E)$ for $(a) \neq (0)$ in a neighbourhood $\mathfrak{A}$ of (0). Take $\mathfrak{A}$ so small that the arcs (3.4) lie in the given field. Define $\mathfrak{F}$ to be all (a, y) of the field whose projections (a) lie in $\mathfrak{A}$. Consider any admissible C in $\mathfrak{F}$ which satisfies (2.3). The components (a) of C determine an arc of the family (3.4) with the same end points as C. From the invariance of I^*, $I^*(C) = I^*(a) > I^*(E)$, the equality holding in case C and E have the same (a).

The next theorem deals with a Mayer field for the second variation I_2. Since I_2 is non-parametric, to describe a field for this integral requires a slight modification of the definition of a field already given. For the second variation the slope functions π_i of the field are functions of (t, a, η) and the invariant integral has the form (3.3). With this in mind we state the next theorem; we omit the proof which is similar to that found in [5, p. 316].

THEOREM 3.3 *Let* E *be an extremal of a field which satisfies the end conditions* (2.3). *Then the set of points* (t, a, η) *with* $t_1 \leqslant t \leqslant t_2$ *and* (a, η) *arbitrary, and the slope functions*

$$\pi_i(t, a, \eta) = p_{ia_k} a_k + p_{i\eta_j} \eta_j$$

define an accessory Mayer field for the second variation I_2 *of* I *along* E *subject to the end conditions* (2.12). *The Hilbert integral for this accessory field is the integral* I_2^* *given by* (3.3).

4. Construction of a field. The main result of this section is Theorem 4.1 in which we construct a Mayer field containing a given extremal E. We first establish four lemmas. Throughout the section we *assume that E is represented with arc-length as parameter*. Thus $y'_i y'_i \equiv 1$ and y_i is of class C^4.

LEMMA 4.1. *Let E be an extremal such that $I_2 > 0$ for every admissible variation $(0, \eta)$ satisfying (2.12). Then E has on it no point conjugate to the initial point.*

Suppose P_3, corresponding to $t = t_3$, is conjugate to the initial point P_1. Then there exists a special accessory extremal $(0, \eta)$ vanishing at t_1 and t_3 but not identically on t_1t_3. Define $(\bar{\eta})$ as (η) on t_1t_3 and (0) on t_3t_2. Then

$$I_2(0,\eta) = \int_{t_1}^{t_3} [\bar{\eta}_i \omega_{\eta_i} + \bar{\eta}'_i \omega_{\eta' i}] dt$$

$$= \int_{t_1}^{t_3} \left[\eta_i \frac{d}{dt} \omega_{\eta' i} + \eta'_i \omega_{\eta' i} \right] dt = [\eta_i \omega_{\eta' i}]_{t_1}^{t_3} = 0.$$

Thus $\eta_i = w y'_i$. Multiplying both sides of the last equation by y'_i and summing we obtain $w = \eta_i y'_i$; thus w is of class C' on t_1t_3. Hence we may differentiate with respect to t in the preceding equation for (η). Doing this, multiplying by y'_i, and summing, we find $w' = k =$ constant, by (2.14). Thus $w = kt + l$. Hence, since w vanishes at t_1 and t_3, it vanishes identically on t_1t_3. The same then holds for (η), contrary to an earlier statement in the proof.

LEMMA 4.2. *Let E be a non-singular extremal which satisfies the end conditions (2.3). Suppose E has on it no point conjugate to the initial point. Then there exist functions $b_i(a), c_i(a)$ defined and of class C'' in a neighbourhood of the value $(a) = (a_0)$ belonging to E such that when b_i, c_i are replaced by $b_i(a), c_i(a)$ in (2.5) the resulting family of extremals*

$$a_h,\ y_i(t,a) = y_i(t, a, b(a), c(a)) \tag{4.1}$$

satisfies (2.3). Also $b_i(a_0), c_i(a_0)$ are the values (b_0, c_0) belonging to E.

To establish this result we show first that the determinant

$$\begin{vmatrix} y_{\omega_i}(t_1) & y_{\varepsilon_i}(t_1) \\ y_{\omega_i}(t_2) & y_{\varepsilon_i}(t_2) \end{vmatrix}$$

is different from zero (the arguments not displayed belong to E). Assume the contrary. Then for some constant $(r, s) \neq (0,0)$, the admissible variation

$$a_h = 0, \quad \eta_i = r_i y_{\omega_i} + s_i y_{\varepsilon_i}$$

would vanish at t_1 and t_2. Furthermore this variation would be a special accessory extremal as one can verify by substituting (2.5) into (2.4) and (2.6) and differentiating. Since P_2 is not conjugate to P_1 we would have $\eta_i \equiv 0$, contrary to the fact that the determinant (2.7) is different from zero along E. Consider now the equations

$$y_{i1}(a) = y_i(t_1, a, b, c),$$
$$y_{i2}(a) = y_i(t_2, a, b, c).$$

They have initial solutions $(a, b, c) = (a_0, b_0, c_0)$, and the functional determinant with respect to (b, c) does not vanish there. By the implicit function theorem the solutions $b_i = b_i(a)$, $c_i = c_i(a)$ of these equations will then satisfy the conclusion of the theorem.

LEMMA 4.3. *Let E satisfy the hypotheses of Lemma 4.2. Then the admissible variations*

$$a_{hk} = \delta_{hk}, \quad \eta_{ik}(t) = y_{ia_k}(t, a_0) \qquad (k = 1, 2, \ldots, r),$$

derived from (4.1), form a set of r special accessory extremals which satisfy (2.12).

For the proof we need only substitute the family (4.1) into equations (2.3), (2.4), and (2.6) and differentiate.

LEMMA 4.4. *Let E satisfy the hypotheses of Lemma 4.2. Then there exists a conjugate system*

$$a_{hp} = 0, \quad u_{ip}(t) \qquad (p = 1, 2, \ldots, n-1)$$

of special accessory extremals which satisfy on $t_1 t_2$ the conditions

$$|u_{ip}(t)\, y'_i(t)| \not\equiv 0, \quad y'_i(t) u_{ip}(t) = 0. \tag{4.2}$$

For the proof let P_1 and P_2 be the left and right end points of E. By standard procedure we can show that there is a point P_3 on the leftward extension of E which has no conjugate point [3, p. 123] between t_1 and t_2. Choose constants e_{ip} such that $e_{ip} y'_i(t_3) = 0$ and $|e_{ip} y'_i(t_3)| \not\equiv 0$. We can choose $n-1$ special accessory extremals $(0, u_p)$ with initial values $u_{ip}(t_3) = 0$, $u'_{ip}(t_3) = e_{ip}$, and the zeros $t \neq t_3$ of the determinant in (4.2) will yield the points on E_{32} conjugate [4] to P_3. Thus the first relation of (4.2) holds. The second relation of (4.2) holds because the left side is constant, by the definition of special accessory extremal, and this constant is zero by the choice of e_{ip}.

We now proceed to the construction of a Mayer field containing E.

THEOREM 4.1. *Let E be a non-singular extremal which does not intersect itself and which satisfies the end conditions (2.3). Suppose E has on it no point conjugate to its initial point. Then there exists an $(r + n - 1)$-parameter family of extremals.*

$$a_h, y_i(t, a, e) \qquad (h = 1, 2, \ldots, r; i = 1, 2, \ldots, n) \tag{4.3}$$

which satisfies the equation $y'_i y''_i = 0$ and which contains the family (4.1) for values $e_p = 0$ $(p = 1, 2, \ldots, n-1)$. The functions y_i, y'_i are defined and of class C'' in a neighbourhood of the values (t, a, e) belonging to E. Also, along E we have

$$y_{ia_k} = \eta_{ik}, \quad y_{ie_p} = u_{ip} \tag{4.4}$$

for the variations of Lemmas 4.3 and 4.4. The extremal E is an extremal of a Mayer field $\mathfrak{F}$ with slope functions

$$p_i(a, y) = y'_i[t(a, y), a, e(a, y)], \tag{4.5}$$

where $t(a, y), e(a, y)$ are the unique solutions of class C'' of the equations

$$y_i = y_i(t,a,e), \tag{4.6}$$

for (a, y) in $\mathfrak{F}$.

In the proof we shall employ the functions and notations of Theorem 2.1 and the previous lemmas. Let

$$B_i(a,e) = b_i(a) + u_{ip}(t_0)e_p,$$

$$v_{ip}(t) = \omega_{y'_i}(0,u_p) \equiv f_{y'_i y_j} u_{jp} + f_{y'_i y'_j} u'_{jp}.$$

Consider the equations

$$f_{y'_i}[a,B(a,c),C]u_{ip}(t_0) = f_{y'_i}[a,b(a),c(a)]u_{ip}(t_0) + v_{iq}(t_0)u_{ip}(t_0)e_q, \tag{4.7}$$

$$C_i C_i = c_i(a)c_i(a).$$

They have initial solutions $(e, a, C) = (0, a, c(a))$ for (a) in a neighbourhood of (a_0). The functional determinant with respect to (C) at $(e, a, C) = (0, a_0, c_0)$ equals

$$2|A_{kj}| \qquad \begin{cases} A_{pj} = f_{y'_i y'_j} u_{ip}(t_0) & (p = 1,2,\ldots,n-1), \\ A_{nj} = y'_j(t_0) & (j,k = 1,2,\ldots,n). \end{cases} \tag{4.8}$$

Suppose this determinant were zero. Then there would exist constants m_p, m not all zero such that

$$m_p f_{y'_i y'_j} u_{ip} + m_0 y'_j = 0.$$

Multiplying by y'_j and summing, $m_0 = 0$. From non-singularity, $m_p u_{ip} = w y'_i$ for some number w. From Lemma 4.4, $m_p = w = 0$; contradiction. By continuity the functional determinant is different from zero for $(e, a, C) = (0, a, c(a))$ with (a) in a neighbourhood of (a_0). We can then solve equations (4.7) for $C_i = C_i(a, e)$, where these functions are defined and of class C'' near $(a_0, 0)$ and have the value $c_i(a)$ for $(e) = (0)$.

The family extremals (4.3) will be shown to be

$$a_h, \quad y_i(t,a,e) = y_i[t, a, B(a,e), C(a,e)].$$

The first of equations (4.4) follows from Lemma 4.3 and the fact that for $(e) = (0)$ this family is (4.1). To prove the second of equations (4.4), we note first by Theorem 2.1 that

$$y_i(t_0,a,e) = B_i(a,e) = b(a) + u_{ip}(t_0)e_p, \tag{4.9}$$

$$y'_i(t_0,a,e) = C_i(a,e).$$

Setting $C_i = C_i(a, e)$ in equations (4.7), differentiating with respect to e_q, and setting $(a, e) = (a_0, 0)$ we obtain

$$(f_{y'_i y_j} B_{je_q} + f_{y'_i y'_j} C_{je_q})u_{ip} = v_{iq}u_{ip}, \qquad C_j C_{je_q} = 0.$$

With the help of (4.9) and the definition of v_{iq} these equations become

$$f_{y'_i y'_j} u_{ip} \quad (C_{je_q} - u'_{jq}) = 0, y'_j C_{je_q} = 0.$$

The last equation and (4.2) imply that

$$y'_i(C_{js_\alpha} - u'_{jq}) = 0.$$

But the determinant (4.8) does not vanish. Hence

$$C_{js_\alpha} - u'_{jq} = 0.$$

The last equation and differentiation of (4.9) yield

$$y_{is_\beta}(t_0,a_0,0) = u_{ip}(t_0),$$

$$y'_{is_\beta}(t_0,a_0,0) = C_{is_\beta}(a_0,0) = u'_{ip}(t_0).$$

By substituting (4.3) into (2.4) and (2.6) and differentiating with respect to e_p we find that $y_{is_p}(t, a_0, 0)$ is a special accessory extremal with $(\alpha) = (0)$. But such an accessory extremal is uniquely determined by the values (η, η') at a single point. This establishes the second of equations (4.4).

Next consider the equations (4.6). They have solutions (y, t, a, e) for the values belonging to E. Furthermore, no two such distinct points have the same projection (y, a), and the functional determinant along E with respect to (t, e) is the determinant (4.2). Hence solutions $t = t(a, y)$, $e_p = e_p(a, y)$ exist, defined and of class C'' in a neighbourhood $\mathfrak{F}$ of the values (a, y) belonging to E. Therefore the slope functions (4.5) are well defined and E is an extremal of the field $\mathfrak{F}$. It remains to show the invariance of the Hilbert integral. On the hypersurface a_h = constant, $y_i = y_i(t_0, a, e)$ this integral becomes

$$\begin{aligned}
&\int f_{y'_i}[a,\ (t_0,a,e),\ y'(t_0,a,e)]y_{is_p}(t_0,a,e)de_p \\
&\qquad = \int f_{y'_i}[a,\ B(a,e),\ C(a,e)]u_{ip}(t_0)de_p \\
&\qquad = \int \{f_{y'_i}[a,\ b(a),\ c(a)]u_{ip}(t_0) + v_{iq}(t_0)u_{ip}(t_0)e_q\}de_p \\
&\qquad = \int d[f_{y'}u_{ip}e_p + \tfrac{1}{2}v_{iq}u_{ip}e_qe_p],
\end{aligned}$$

by use of (4.7) and (2.15). From the invariance on the hypersurface follows [3, p. 126] the invariance in $\mathfrak{F}$.

THEOREM 4.2. *Let E be a non-singular extremal which does not intersect itself and which satisfies the end conditions* (2.3). *Suppose that the second variation of I along E is positive. Let*

$$\pi_i(t,a,\eta) = \eta'_{ik}a_k + u'_{ip}\epsilon_p + y''_i\tau, \tag{4.10}$$

where $\epsilon_p = \epsilon_p(t,a,\eta)$, $\tau = \tau(t,a,\eta)$ are the unique solutions of the equations

$$\eta_i = \eta_{ik}a_k + u_{ip}\epsilon_p + y'_i\tau. \tag{4.11}$$

Then the functions π_i are the slope functions of the accessory Mayer field associated with the field $\mathfrak{F}$ described in the preceding theorem. Furthermore, the invariant integral I_2^* of the accessory field satisfies the condition $I_2^*(a, \eta) > 0$ for every admissible variation with $(a) \neq (0)$ satisfying (2.12).

Using Lemma 4.1 and Theorems 4.1 and 3.3 we obtain (4.10) as the slope functions of the accessory field, where

$$e_p = e_{pa_k}a_k + e_{py_j}\eta_j, \qquad \tau = t_{a_k}a_k + t_{y_j}\eta_j.$$

In the identity $y_i = y_i[t(a, y), a, e(a, y)]$ replace (a, y) by $(a, y) + b(a,\eta)$, differentiate with respect to b, and set $b = 0$. The result is (4.11). To prove the last part of the theorem let (a, η) be any admissible variation as described in the theorem. Then $a, \bar{\eta} = a_k\eta_k$ has the same end points; from equations (4.11) and (4.10) this variation is an extremal of the accessory field. Therefore

$$I_2^*(a,\eta) = I_2^*(a,\bar{\eta}) = I_2(a,\bar{\eta}) > 0.$$

5. Proof of Theorem 2.2. We are now in a position to prove Theorem 2.2. Imbed E in the field described in Theorem 4.1. From Theorem 4.2 the hypotheses of Theorem 3.2 are satisfied. Hence there exists a neighbourhood $\mathfrak{F}$ of E with the properties described there. Pick a neighbourhood N of non-singular elements (a, y, y') for which the Weierstrass condition holds. By a theorem of Hestenes and Reid [7] the strict inequality holds in the Weierstrass condition. Decrease the field if necessary so that the elements $a, y, p(a, y)$ all lie in N. Then the hypotheses of Theorem 3.1 are satisfied and our proof is complete.

For use in the study of the isoperimetric problem we shall need the following two theorems.

THEOREM 5.1. *Let E be a non-singular extremal which does not intersect itself and satisfies the end conditions* (2.3). *Suppose that E satisfies the Weierstrass condition II_N and has on it no point conjugate to its initial point. Then there exists a field $\mathfrak{F}$ containing E as an extremal of the field such that the E-function is positive in $\mathfrak{F}$. Furthermore, if (a) is sufficiently close to the value (a_0) belonging to E then there exists a unique extremal in $\mathfrak{F}$ with components a_h which satisfies* (2.3). *This extremal is an extremal of the field.*

As in the preceding proof we select a neighbourhood in which the strengthened Weierstrass condition holds. From Theorem 4.1 we obtain a field $\mathfrak{F}$ containing E with all its elements $[a, y, p(a, y)]$ in N. This proves the first part of the theorem. To show the existence of an extremal for every value (a) we exhibit $(a, y\ (t, a, 0))$ of (4.3). Furthermore, this extremal is an extremal of the field described in Theorem 4.1. The uniqueness follows from the last statement of Theorem 2.1 and the proof of Lemma 4.2.

The proof of the next theorem is like that of Theorem 3.1.

THEOREM 5.2. *Let E be an extremal of a Mayer field $\mathfrak{F}$ at each point of which $E[a, y, p(a, y), y'] > 0$ for $(y') \neq (kp)$, $k > 0$, with (a, y, y') admissible. Then*

$I(C) > I(E)$ for every admissible arc C in $\mathfrak{F}$ with the same end values (a, y_s) as E, the equality holding only in case C is identical with E.

6. The isoperimetric problem. We turn now to the problem of minimizing the function I of (2.1) in the class of admissible arcs (2.2) which satisfy conditions

$$y_i(t_s) = y_{is}(a) \qquad (s = 1,2), \tag{6.1a}$$

$$I_p(C) = g_p(a) + \int_{t_1}^{t_2} f_p(a,y,y')dt = 0 \qquad (p = 1,2,\ldots,m). \tag{6.1b}$$

This problem differs from the earlier one in the adjunction of the isoperimetric side conditions (6.1b). We shall assume that the functions f, f_p are positively homogeneous of degree one in the variables y'_i and that the functions appearing above have the same continuity properties that were assumed earlier.

Associated with this problem is an integral,

$$J(C,l) = G(a,l) + \int_{t_1}^{t_2} F(a,l,y,y')dt, \tag{6.2}$$

where $G(a, l) = g(a) + l_p g_p(a)$, $F(a, l, y, y') = f(a, y, y') + l_p f_p(a, y, y')$ and the l's are constants. We shall employ the function (6.2) to relate the theory of the previous pages to the present case.

By an *isoperimetric extremal* E will be meant an admissible arc (2.2) of class C'' together with a set of constant multipliers l_p $(p = 1, 2, \ldots, m)$ which satisfies the Euler-Lagrange equations

$$F_{y_i} - \frac{d}{dt} F_{y'_i} = 0. \tag{6.3}$$

The conditions of non-singularity and transversality, and the Weierstrass and Clebsch conditions are, with a minor exception, identical with those of §2 provided that in the earlier definitions the functions f, g are replaced by F, G. The exception concerns the Weierstrass condition Π_N. This should be slightly reworded as follows: for every element (a, l, y, y') in a neighbourhood N of those belonging to the arc E, $E(a, l, y, y', Y') \geqslant 0$ for $(Y') \neq (ky')$, $k > 0$, with (a, y, Y') admissible.

The second variation I_2 of I along E is given by (2.10) where the left sides of equations (2.11) are understood now to be defined by the right sides with f, g replaced by F, G. We retain the same notations for the left sides. We shall say that I_2 is *positive* in case $I_2(a, \eta) > 0$ for every non-tangential admissible variation which satisfies along E the conditions

$$\eta_i(t_s) = y_{isk}a_k \qquad (s = 1,2), \tag{6.4a}$$

$$I_{p1}(a,\eta) = g_{pk}a_k + \int_{t_1}^{t_2} \omega_p(t,a,\eta,\eta')dt \qquad (p = 1,2,\ldots,m), \tag{6.4b}$$

where

$$\omega_p = f_{pa_k}a_k + f_{py_i}\eta_i + f_{py'_i}\eta'_i.$$

By an *isoperimetric accessory extremal* will be meant an admissible variation (α, η) of class C'' together with constant multipliers λ_ρ which satisfies the accessory differential equations

$$\Omega_{\eta_i} - \frac{d}{dt}\Omega_{\eta'_i} = 0, \tag{6.5}$$

where $\Omega(t, \alpha, \lambda, \eta, \eta') = \omega + \lambda_\rho \omega_\rho$. An isoperimetric accessory extremal which satisfies (2.14) will be called *special*.

Consider an isoperimetric extremal E with multipliers l_ρ. We shall say that t_4 defines a point P_4 *conjugate* to a point P_3 on E relative to the function $J(C, l)$ of (6.2) in case there exists a special isoperimetric accessory extremal with $(\alpha) = 0, (\lambda) = 0$ which vanishes at t_3 and t_4 but is not identically zero on $t_3 t_4$.

Our main objective is the sufficiency theorem below. Notice that there are no normality restrictions in this result. Our method of proof will consist of proving the theorem under the assumption of "strong normality" and then showing how this restriction may be dropped.

THEOREM 6.1. *If a non-singular isoperimetric extremal E_0 which does not intersect itself satisfies the conditions* (6.1), *the transversality condition, the Weierstrass condition* Π_N, *and is such that the second variation of I along E_0 is positive, then there exists a neighbourhood* $\mathfrak{F}$ *of E in ay-space such that $I(C) > I(E_0)$ for every admissible arc C in* $\mathfrak{F}$ *satisfying* (6.1) *but not identical with E_0.*

7. A generalization of the Hahn lemma. We first establish the usual type of Hahn lemma.

THEOREM 7.1. *Let E_0: $(a_0, y_0(t))$ be a non-singular isoperimetric extremal with multipliers (l_0) which does not intersect itself. Suppose E_0 satisfies the Weierstrass condition* Π_N *and E_0 has on it no point conjugate to its initial point relative to $J(C, l_0)$. Then there exist neighbourhoods* $\mathfrak{F}$ *of E_0 in ay-space and* $\mathfrak{L}$ *of the multipliers (l_0) such that for every pair of points in* $\mathfrak{F}$ *sufficiently close to the initial and terminal points respectively of E_0, and every set of multipliers in* $\mathfrak{L}$ *there is a unique isoperimetric extremal E_l in* $\mathfrak{F}$ *with these end points and multipliers. Furthermore, $J(C, l) > J(E_l, l)$ for every admissible arc C in* $\mathfrak{F}$ *joining the end points of E_l but not identical with it. Also, for every sub-arc $\bar{E}_l$ of E_l we have $J(C, l) > J(\bar{E}_l, l)$ for every admissible arc C in* $\mathfrak{F}$ *joining the end points of $\bar{E}_l$ but not identical with it.*

To make the proof consider the problem of minimizing the function (6.2) in the class of admissible arcs

$$a_h, l_\rho, y_{i1}, y_{i2}, y_i(t)$$

which satisfy end conditions of the form

$$y_i(t_s) = y_{is}.$$

This is a non-isoperimetric problem with the constants a_h replaced by a_h, l_ρ, y_{is}. For this problem the arc defined by the values belonging to E_0 satisfies the

hypotheses of Theorem 5.1. The conclusions of Theorems 5.1 and 5.2 appropriately interpreted yield the desired result.

Consider now an arc E_0 satisfying the hypotheses of Theorem 7.1 with the exception of the assumption on conjugate points. We proceed to make the following geometric construction for such an arc. It is a standard result in the calculus of variations that there exists a positive constant d so small that no sub-arc of E_0 of length not exceeding d has on it a pair of conjugate points relative to $J(C, l_0)$. Let $Q_0, Q_1, \ldots, Q_{q+1}$ be successive points on E_0 such that the arcs Q_jQ_{j+2} do not exceed d in length. We may suppose that the points Q_0 and Q_{q+1} lie respectively on the leftward and rightward extensions of the arc E_0, and that the initial point P_1 of E_0 lies between Q_0 and Q_1 while the terminal point P_2 lies between Q_q and Q_{q+1}. Through the points Q_j pass hyperplanes π^j cutting E_0 orthogonally. By Theorem 7.1 we can select a neighbourhood $\mathfrak{F}''$ of E_0 and $\mathfrak{L}'$ of (l_0) such that, for every pair of points R_j, R_{j+2} with the same components (a) on π^j, π^{j+2} sufficiently close to Q_j, Q_{j+2} respectively and every (l) in $\mathfrak{L}'$, there is a unique isoperimetric extremal E in $\mathfrak{F}''$ with multipliers (l) and end points R_j, R_{j+2} which affords $J(C, l)$ a proper minimum relative to admissible arcs C in $\mathfrak{F}''$ joining the points R_j, R_{j+2} and not crossing the manifolds π^j, π^{j+2}. Let $\mathfrak{F}'$ be a neighbourhood of E_0 contained in $\mathfrak{F}''$, and $\mathfrak{L}$ a neighbourhood of (l_0) contained in $\mathfrak{L}'$ such that every pair of points R_j, R_{j+1} in $\mathfrak{F}'$ with the same components (a) and lying on π^j, π^{j+1} respectively determines together with a set (l) in $\mathfrak{L}$ an isoperimetric extremal E in $\mathfrak{F}''$ with end points on π^{j-1}, π^{j+2} and multipliers (l) such that E has the following property: the arc E intersects each of π^j, π^{j+1} exactly once, at the points R_j, R_{j+1}. Thus the segment E_j of E between these points does not cross π^j, π^{j+1}. Also, by Theorem 7.1, E_j will afford $J(C, l)$ a proper minimum relative to admissible arcs C in $\mathfrak{F}''$ joining the points R_j, R_{j+1} and not crossing π^{j-1}, π^{j+2}. Let π_0 be the end manifold in ay-space determined by $a_h = a_h$, $y_i = y_{is}(a)$ for $s = 1$ and π_{q+1} the manifold for $s = 2$. Let π_j denote π^j $(j = 1, 2, \ldots, q)$. Then we may require that the neighbourhoods $\mathfrak{F}'$ and $\mathfrak{L}$ also satisfy the following condition: for every pair of points R_0, R_1 in $\mathfrak{F}'$ with the same components (a) and lying on π_0, π_1 respectively and every (l) in $\mathfrak{L}$ there is an isoperimetric extremal in $\mathfrak{F}''$ with multipliers (l) and end points R_0, R_1 which does not cross π_1 and affords $J(C, l)$ a proper minimum relative to admissible arcs C in $\mathfrak{F}''$ joining R_0, R_1 but not crossing π_1. A similar result holds for points R_q, R_{q+1} in $\mathfrak{F}'$ on π_q, π_{q+1}. Finally, we may restrict $\mathfrak{F}'$ to include no points of $\mathfrak{F}''$ to the left of π^0 or to the right of π^{q+1}. We are now in a position to state the following important result.

THEOREM 7.2. *Let E_0 be a non-singular isoperimetric extremal which does not intersect itself and satisfies the Weierstrass condition II_N. Let the neighbourhoods $\mathfrak{F}''$, $\mathfrak{F}'$, $\mathfrak{L}$ and the manifolds π_j be defined as in the above paragraph. Then every pair of points R_j, R_{j+1} in $\mathfrak{F}'$ with the same components a_h and lying on the manifolds π_j, π_{j+1} respectively determines together with a set of multipliers l_p in $\mathfrak{L}$ a unique isoperimetric extremal E_j in $\mathfrak{F}''$ with these end points and multipliers such*

that $J(C, l) > J(E_j, l)$ for every admissible arc C in $\mathfrak{F}'$ joining the end points of E_j and not identical with E_j.

It remains only to prove the asserted inequality. Let C be an admissible arc in $\mathfrak{F}'$ joining the end points of E_j. If C does not cross the hyperplanes π^j, π^{j+1} then, by our earlier discussion, $J(C, l) > J(E_j, l)$ unless $C \equiv E_j$. Suppose C crosses π^j. Let π^{k-1} be the first hyperplane on the left which C does not cross. As the point P moves along C from R_j to R_{j+1} it will intersect π^k at a first point R_k and will subsequently reach π^{k+1} at a first point R_{k+1}. Let C' be the segment of C between R_k and R_{k+1} and let E be the isoperimetric extremal between π^k and π^{k+1} determined by R_k, R_{k+1} and the multipliers l_p. Then $J(C', l) > J(E, l)$, the strict inequality holding because the arc C' is not identical with E (since C' actually crosses π^k). We replace the sub-arc C' of C by E to obtain a new arc C_1 joining the end points of C for which $J(C, l) > J(C_1, l)$. The arc C_1 may be in $\mathfrak{F}''$ but it crosses the hyperplanes at points in $\mathfrak{F}'$. If the new arc C_1 still crosses the hyperplane π^k we apply our lopping-off process to it. From the finite length of the arc C in a finite number of steps we can replace the original arc C by an arc C_k which does not cross π^k and for which $J(C, l) > J(C_k, l)$. In a similar fashion we obtain an arc C_{k+1} which does not cross π^{k+1} and, finally, an arc C_2 which does not cross π^j and satisfies the inequality $J(C, l) > J(C_2, l)$. Proceeding in an analogous manner to the right of the hyperplane π^{j+1} we eventually obtain an admissable arc C_3 in $\mathfrak{F}''$ which joins the end points of E_j and does not cross π^j, π^{j+1}. Hence

$$J(C,l) > J(C_3,l) \geqslant J(E_j,l)$$

and the proof is complete.

By an argument like that above we can establish the following extension of Theorem 7.1.

THEOREM 7.3. *Let E_0 satisfy the hypotheses of Theorem 7.2 with multipliers (l_0). Suppose $\bar{E}_0$ is a sub-arc of E_0 which has on it no pairs of conjugate points. Then there exists a neighbourhood $\mathfrak{F}$ of E_0 in ay-space and a neighbourhood $\mathfrak{L}$ of (l_0) such that every pair of points (a, y_1) and (a, y_2) sufficiently close to the initial and terminal points respectively of $\bar{E}_0$ and every set l_p in $\mathfrak{L}$ determine a unique isoperimetric extremal with these end points and multipliers which affords the function $J(C, l)$ a proper minimum relative to admissible arcs joining its end points and lying in $\mathfrak{F}$.*

8. Proof of Theorem 6.1 in the strongly normal case. We introduce at this point the notion of normality. We shall say that an isoperimetric extremal E is *normal* relative to the isoperimetric conditions (6.1b) if there do not exist constants c_p not all zero such that the following equations hold along E.

$$c_p\left(f_{py_i} - \frac{d}{dt} f_{py'_i}\right) = 0, \tag{8.1}$$

$$c_p\left(dg_p + [f_{py'_i} dy_i]_1^2 + \int_{t_1}^{t_2} f_{a_i} da_i dt\right) = 0.$$

In other words, E is normal in case E is not an extremal satisfying the transversality condition for an integral of the form

$$c_p I_p = c_p g_p(a) + \int_{t_1}^{t_0} c_p f_p dt. \tag{8.2}$$

We shall say that E is *strongly normal* relative to the isoperimetric conditions (6.1b) if there do not exist constants c_p not all zero such that the first of equations (8.1) holds or, equivalently, the arc E is not an extremal for a function (8.2). Obviously strong normality implies normality. Equations (8.1) are equivalent to the condition that the first variation

$$c_p I_{p1}(a,\eta) \tag{8.3}$$

of (8.2) along E vanishes for all admissible variations satisfying (6.4a). Similarly, the first equation (8.1) is equivalent to the vanishing of (8.3) for all such variations with $(a) = (0)$.

In the proof of Theorem 6.1 we shall make use of the following result.

THEOREM 8.1. *Let E_0 be an arc, satisfying the hypotheses of Theorem* 6.1, *which is strongly normal with respect to the isoperimetric conditions* (6.1b). *Let the neighbourhoods $\mathfrak{F}'$ and $\mathfrak{L}$ and the manifolds π_j be defined as in Theorem* 7.2. *Then there exists a neighbourhood $\mathfrak{F}$ of E_0 contained in $\mathfrak{F}'$ such that for every succession of points $R_0, R_1, \ldots, R_q, R_{q+1}$ in $\mathfrak{F}$ with the same components a_h and lying on successive manifolds $\pi_0, \pi_1, \ldots, \pi_q, \pi_{q+1}$ there is a set of multipliers*

$$l_p = l_p(R_0, \ldots, R_{q+1})$$

in $\mathfrak{L}$ such that the broken isoperimetric extremal E determined by the points R_j and the multipliers l_p by means of Theorem 7.2 *satisfies conditions* (6.1) *and the inequality $I(E) \geqslant I(E_0)$, the equality holding only in case E is identical with E_0.*

If one accepts for the moment the truth of this theorem then the proof of Theorem 6.1 under the assumption of strong normality may be made as follows. Let $\mathfrak{F}$ be the neighbourhood given in Theorem 8.1. Consider any admissible arc C in $\mathfrak{F}$ satisfying the conditions (6.1). Let R_0, R_{q+1} be the initial and terminal points of C and let R_j $(j = 1, 2, \ldots, q)$ be the last point at which the point P crosses the hyperplane π_j as P moves along C from its initial to its terminal point. Let E be the broken isoperimetric extremal of Theorem 6.1 determined by the points $R_0, \ldots, R_{q+1}$ and the multipliers $l_p = l_p(R_0, \ldots, R_{q+1})$. Denote by C_j the segment of C between R_j and R_{j+1}, and by E_j the segments of E between R_j and R_{j+1}. Then by Theorems 7.2 and 8.1, and equations (6.1b) we obtain

$$\begin{aligned} 0 \leqslant \sum_j [J(C_j,l) - J(E_j,l)] &= J(C,l) - J(E,l) \\ &= I(C) - I(E) \leqslant I(C) - I(E_0), \end{aligned}$$

the equality holding only in case C is identical with E_0.

Let us turn now to the proof of Theorem 8.1. Let

$$t_1 = s_0 < s_1 < \ldots < s_q < s_{q+1} = t_2$$

be the parametric values which determine the points of intersection of E_0 with the manifolds $\pi_0, \pi_1, \ldots, \pi_{q+1}$. Let the equations of the hyperplanes π_j $(j = 1, 2, \ldots, q)$ be

$$a_h = a_h, \quad y_i = b_{ij}(e_{1,j}, e_{2,j}, \ldots, e_{n-1,j}) \quad (h = 1,2,\ldots,r;\ i = 1,2,\ldots,n) \tag{8.4}$$

(j not summed). Along E_0

$$y_{i0}(s_0) = y_{i1}(a_0), \quad y_{ip}(s_j) = b_{ij}(e_{j0}), \quad y_{i0}(s_{q+1}) = y_{i2}(a_0). \tag{8.5}$$

Also, we have the orthogonality conditions

$$y'_{i0}(s_j)\frac{\partial b_{ij}}{\partial e_{kj}} = 0 \qquad (k = 1,2,\ldots,n-1; \quad j \text{ not summed}). \tag{8.6}$$

Moreover, for each j, the matrix

$$\left\| \frac{\partial b_{ij}}{\partial e_{kj}} \right\|$$

has rank $n - 1$ at $(e_j) = (e_{j0})$. By means of Theorem 7.1 and its proof we can obtain the existence of an $(h + nq + m)$-parameter family of broken isoperimetric extremals

$$a_h, \ y_i = Y_i(t, a_1, \ldots, a_h, b_{11}, \ldots, b_{nq}, l_1, \ldots, l_m) \tag{8.7}$$

with multipliers (l) which satisfies the following conditions. It contains E_0 for values (a_0, b_0, l_0), and $t_1 \leqslant t \leqslant t_2$. Except possibly at the corner points $t = s_j$ $(j = 1, 2, \ldots, q)$ the functions Y_i, Y_{it} are of class C'' in a neighbourhood of the values (t, a, b, l) belonging to E_0. For fixed values (a, b, l) the corresponding arc of the family satisfies the end conditions (6.1a) and passes through the point (a, b_j), for $t = s_j$ $(j = 1, 2, \ldots, q)$. Finally, the identity

$$Y_{it}Y_{itt} = 0 \tag{8.8}$$

holds. Replacing the arguments in (8.7) by the functions of (8.4) we obtain a family

$$a_h, \ y_i = y_i(t,a,e,l) \tag{8.9}$$

of broken isoperimetric extremals with multipliers (l). This is the family determined by a sequence of points $R_0, \ldots, R_{q+1}$ on the manifolds $\pi_0, \ldots, \pi_{q+1}$. Substitute (8.9) into (6.1b) to obtain

$$I_p(a,e,l) = 0. \tag{8.10}$$

Equations (8.10) have an initial solution (a_0, e_0, l_0) and the functions on the left are of class C''. Assume for the moment that the functional determinant

$$\left\| \frac{\partial I_p}{\partial l_k} \right\| \qquad (p,k = 1,2,\ldots,m) \tag{8.11}$$

is different from zero at the initial solution. Then (8.10) has unique solutions $l_p = l_p(a, e)$ of class C'' near (a, e_0) with $l_p(a_0, e_0) = l_{p0}$. Let (a, e) define the sequence of points $R_0, \ldots, R_{q+1}$. We shall show that the functions $l_p(R)$ of the theorem are the functions $l_p(a, e)$.

The family

$$a_h,\ y_i(t, a, e) = y_i[t, a, e, l(a,e)] \tag{8.12}$$

with the indicated multipliers satisfy (6.1). It remains only to show that E_0 affords I a proper minimum relative to arcs of (8.12). Consider the variation $(da, \delta y(t))$ where

$$\delta y_i(t) = y_{ia_h}(t,a_0,e_0)da_h + \frac{\partial y_i(t,a_0,e_0)}{\partial e_{kj}}de_{kj}.$$

From the equations

$$y_i(s_0,a,e) = y_{i1}(a), \quad y_i(s_j,a,e) = b_{ij}(e_{kj}), \quad y_i(s_{q+1},a,e,) = y_{i2}(a)$$

(j not summed) we obtain

$$\delta y_i(s_0) = y_{i1a}da_h, \quad \delta y_i(s_j) = \frac{\partial b_{ij}}{\partial e_{kj}}de_{kj}, \quad \delta y_i(s_{q+1}) = y_{i2a}da_h. \tag{8.13}$$

These relations together with differentiation of the identity

$$I_p(a, e) = I_p[a, e, l(a,e)] = 0$$

yield that $(da, \delta y)$ satisfies (6.4) and has $(\delta y) \equiv 0$ only if $de_{kj} = 0$ for all k, j. Suppose this variation is of the tangential form $(0, wy'_0)$. Then, by an argument like that used in the proof of Lemma 4.1, $w(t)$ is linear on each sub-interval $s_j s_{j+1}$. But multiplying $\delta y_i(s_j) = w(s_j)y'_{i0}(s_j)$ by $y'_{i0}(s_j)$, summing, and employing (8.6) and (8.13) we find

$$w(s_j) = 0 \qquad (j = 0,1, \ldots, q+1).$$

Hence $w(t) \equiv 0$, $(\delta y) \equiv 0$, and finally $(de) = 0$. Therefore for $(da, de) \not\equiv (0,0)$ the variation $(da, \delta y)$ is not tangential and hence $I_2(da, \delta y) > 0$. Consider now the function $J(a, e, l_0)$ obtained by evaluating the integral $J(C, l_0)$ along (8.12). By computation we find that along E_0 the relations

$$dJ = dG + [F_{y'_i}dy_i]_1^2 + \int_{t_1}^{t_2} F_{a_h}da_h dt = 0,$$

$$d^2J = I_2(da,\delta y) > 0,$$

for all $(da, de) \not\equiv (0,0)$. Hence for (a, e) near, but distinct from, (a_0, e_0)

$$0 < J(a,e,l) - J(a_0,e_0,l_0) = I(a,e) - I(E_0)$$

since $I_p(a, e) = 0$.

It remains to establish the non-vanishing of (8.11). Let

$$\bar{\delta}y(t) = y_{il_h}(t,a_0,e_0,l_0)dl_h.$$

By differentiating the functions $I_p(a, e, l)$ we find

$$\frac{\partial I_p}{\partial l_k}\, dl_k = I_{p1}(0,\bar{\delta}y). \tag{8.14}$$

Differentiation of the equations

$$y_i(s_0,a,e,l) = y_{i1}(a), \quad y_i(e_j,a,e,l) = b_{ij}(e_j), \quad y_i(s_{q+1},a,e,l) = y_{i2}(a)$$

yields $(\bar{\delta}y(s_j)) = (0)$ $(j = 0, 1, \ldots, q+1)$. Substituting (8.9) into the Euler-Lagrange equations (6.3), differentiating with respect to l_k, multiplying by dl_k and summing we see that

$$\omega_{\eta_i}(0,\bar{\delta}y) - \frac{d}{dt}\,\omega_{\eta'_i}(0,\bar{\delta}y) + dl_k\left(f_{k\eta_i} - \frac{d}{dt} f_{k\eta'_i}\right) = 0. \tag{8.15}$$

Suppose now that (8.11) is zero. Then there exist constants $(dl) \neq 0$ such that the left member of (8.14) vanishes. Hence $(0, \bar{\delta}y)$ satisfies (6.4). This variation is not tangential; otherwise it would satisfy (2.13), which is impossible by (8.15) and our assumption of strong normality. Hence $I_2(0, \bar{\delta}y) > 0$. But by (8.15)

$$\begin{aligned} 0 &= \int_{t_1}^{t_2}\left[\bar{\delta}y_i\left\{\omega_{\eta_i}(0,\bar{\delta}y) - \frac{d}{dt}\omega_{\eta'_i}(0,\bar{\delta}y)\right\} + \bar{\delta}y_i\left\{dl_k\left(f_{k\eta_i} - \frac{d}{dt} f_{k\eta'_i}\right)\right\}\right]dt \\ &= \int_{t_1}^{t_2}\Big[(\bar{\delta}y_i\omega_{\eta_i} + \bar{\delta}y'_i\omega_{\eta'_i}) + dl_k(f_{k\eta_i}\bar{\delta}y_i + f_{k\eta'_i}\bar{\delta}y'_i) \\ &\qquad - \frac{d}{dt}(\omega_{\eta'_i}\bar{\delta}y_i + dl_k f_{k\eta'_i}\bar{\delta}y_i)\Big]dt \\ &= I_2(0,\bar{\delta}y) + dl_k I_{k1}(0,\bar{\delta}y) - \sum_j \int_{s_j}^{s_{j+1}} \frac{d}{dt}(\omega_{\eta'_i}\bar{\delta}y_i + dl_k f_{k\eta'_i}\bar{\delta}y_i)dt \\ &= I_2(0,\bar{\delta}y). \end{aligned}$$

This contradiction completes the proof.

9. The general case. We shall establish the following result.

THEOREM 9.1. *Let E_0 be an arc satisfying the hypotheses of Theorem* 6.1 *for the function* (2.1) *with the side conditions* (6.1). *Then there exists a function*

$$\bar{I}(C) = \bar{g}(a) + \int_{t_1}^{t_2} \bar{f}(a,y,y')dt \tag{9.1}$$

and a set of isoperimetric conditions

$$\bar{I}_\tau(C) = \bar{g}_\tau(a) + \int_{t_1}^{t_2} \bar{f}_\tau(a,y,y')dt \qquad (\tau = 1,2,\ldots,m_1 \leqslant m) \tag{9.2}$$

such that E_0 is strongly normal relative to the conditions (9.2) *and satisfies the hypotheses of Theorem* 6.1 *for the function* (9.1) *with end conditions* (6.1a) *and isoperimetric conditions* (9.2). *Furthermore, if $I(E_0)$ is a proper strong relative minimum for the modified problem, $I(E_0)$ is a similar minimum for the original problem.*

In view of the proof of Theorem 6.1 made in the last section under the assumption of strong normality, the above theorem establishes Theorem 6.1 in its original form.

To prove the theorem let $l_{p\sigma}$ $(\sigma = 1, 2, \ldots, q \leqslant m)$ be a maximal set of linearly independent multipliers such that E_0 is an extremal for each of the functions $l_{p\sigma}I_p(C)$. Choose $l_{p\tau}$ so that the determinant $|l_{p\sigma}, l_{p\tau}|$ does not vanish. Renumber the subscripts so that $\tau = 1, 2, \ldots, m_1$ and $\sigma = m_1 + 1, \ldots, m$. Let

$$\bar{I}_p = I_\beta l_{\beta p} \qquad (\beta, p = 1,2, \ldots, m).$$

Then in our proof (6.1b) may be replaced by the equivalent

$$\bar{I}_p(C) = 0 \qquad (p = 1,2, \ldots, m). \tag{9.3}$$

(We represent the functions on the left in the form (6.1b) with bars over g and f.) Also, we may take the multipliers (l_0) for E_0 to be (0), by transforming from I to $I + l_{p0}I_p$. The conditions (9.3) fall into two sets,

$$\begin{aligned} \bar{I}_\tau &= 0 \qquad (\tau = 1,2, \ldots, m_1), \\ \bar{I}_\sigma &= 0 \qquad (\sigma = m_1 + 1, \ldots, m). \end{aligned} \tag{9.4}$$

The arc E_0 is strongly normal for the first set while it is an extremal for each function in the second set. For an admissible variation satisfying (6.4a),

$$\begin{aligned} \bar{I}_{\sigma 1}(\alpha,\eta) &= \bar{g}_{\sigma h}\alpha_h + \int_{t_1}^{t_2} (\bar{f}_{\sigma\alpha_k}\alpha_k + \bar{f}_{\sigma y_i}\eta_i + \bar{f}_{\sigma y'_i}\eta'_i)dt \\ &= \bar{g}_{\sigma h}\alpha_h + \left(\int_{t_1}^{t_2} \bar{f}_{\sigma\alpha_k}dt\right)\alpha_h + [\bar{f}_{\sigma y'_i}\eta_i]_{t_1}^{t_2} \\ &= L_\sigma(\alpha), \end{aligned}$$

where L_σ is a linear form in (α) with constant coefficients.

With the aid of the following lemma we will be able to complete the proof of the theorem.

LEMMA 9.1. *There exists a positive constant c such that*

$$I_2(\alpha,\eta) + cL_\sigma(\alpha)\bar{I}_{\sigma 1}(\alpha,\eta) = I_2 + cL_\sigma L_\sigma \tag{9.5}$$

is positive for every admissible variation with $(\alpha) \neq (0)$ *which satisfies* (6.4a) *and*

$$I_{\tau 1}(\alpha,\eta) = 0 \qquad (\tau = 1,2, \ldots, m_1). \tag{9.6}$$

Granting this lemma, we see that

$$\bar{I}(C) = I(C) + cL_\sigma(a - a_0)I_\sigma(C)$$

satisfies Theorem 9.1 with the first set of conditions in (9.4). In particular, the second variation of $\bar{I}$ is (9.5), and to show its positiveness it is sufficient by Lemma 9.1 to consider only non-tangential admissible variations with $(\alpha) = (0)$ which satisfy (6.4a) and (9.6). For such a variation,

$$\bar{I}_{\sigma 1}(\mathfrak{a},\eta) = L_\sigma(\mathfrak{a}) = 0. \tag{9.7}$$

Thus, from the positiveness of I_2 relative to (6.4a), (9.6), and (9.7) we deduce that (9.5) is positive. This completes the proof of Theorem 9.1.

We turn to the proof of the lemma. For this we consider for a moment the linear differential equations

$$\begin{aligned} \Omega_{\eta i} - \frac{d}{dt}\,\Omega_{\eta' i} + \mu y'_{i0} &= 0, \\ y'_{i0}\eta''_i + y''_{i0}\eta'_i &= 0, \end{aligned} \tag{9.8}$$

where $\Omega = \omega + \lambda_r\omega_r$, and

$$\omega_r = \bar{f}_{r a_k}\mathfrak{a}_k + \bar{f}_{r\eta_i}\eta_i + \bar{f}_{r\eta'_i}\eta'_i.$$

From the non-singularity of E_0 we can solve (9.8) for η''_i, μ. The solutions have the form

$$\eta''_i = A_{ik}(t)\mathfrak{a}_k + B_{ir}(t)\lambda_r + C_{ij}(t)\eta_j + D_{ij}(t)\eta'_j \tag{9.9}$$

and $\mu = \mu(\mathfrak{a}, \lambda, \eta, \eta')$. By multiplying the first equation (9.8) by y'_{i0}, summing, and using the homogeneity properties of $f, \bar{f}_r$ and the fact that E_0 is an extremal for the function I we obtain $\mu = 0$. It follows that the solutions $\mathfrak{a}_k, \lambda_r, \eta_i(t)$ of the differential equations (9.9) are precisely the speical accessory (isoperimetric) extremals. From well-known theorems on linear differential equations we obtain the existence of $2n + m_1 + r$ linearly independent solutions

$$\mathfrak{a}_{kj},\ \lambda_{rj},\ \eta_{ij}(t) \qquad (j = 1,2,\ldots,2n + m_1 + r;\quad t_1 \leqslant t \leqslant t_2)$$

of (9.9). Substitute an arbitrary linear combination of these solutions into (9.6) to obtain m_1 linear homogeneous equations in the coefficients c_j. There will be at least $2n + r$ linearly independent solutions c_j of these equations and the correspondingly linearly independent solutions

$$\mathfrak{a}_{kq},\ \lambda_{rq},\ \eta_{iq}(t) \qquad (q = 1,2,\ldots,2n + r) \tag{9.10}$$

of (9.8) will satisfy (9.6). We show that the determinant

$$\begin{vmatrix} \mathfrak{a}_{kq} \\ \eta_{iq}(t_1) \\ \eta_{iq}(t_2) \end{vmatrix} \tag{9.11}$$

does not vanish. Notice that the first equation (9.8) with $\mu = 0$ may be written

$$\omega_{\eta i} - \frac{d}{dt}\omega_{\eta' i} + \lambda_r\left(\bar{f}_{r\eta_i} - \frac{d}{dt}\bar{f}_{r\eta'_i}\right) = 0. \tag{9.12}$$

Suppose now that the determinant is zero. There exist constants c_q, not all zero, such that the special accessory extremal $(0, \eta) = (c_q\mathfrak{a}_q, c_q\eta_q)$ with multi-

pliers $(\lambda) = (c_q\lambda_q)$ satisfies (9.6) and vanishes at the end points. This variation also satisfies (9.7). Since

$$I_2(0,\eta) = \int_{t_1}^{t_2} (\omega_{\eta_i}\eta_i + \omega_{\eta'_i}\eta'_i)dt$$

$$= \int_{t_1}^{t_2} (\omega_{\eta_i}\eta_i + \omega_{\eta'_i}\eta'_i)dt + \lambda_\tau I_{\tau 1}(0,\eta)$$

$$= \int_{t_1}^{t_2} (\Omega_{\eta_i}\eta_i + \Omega_{\eta'_i}\eta'_i)dt = [\Omega_{\eta'_i}\eta^i]_{t_1}^{t_2} = 0,$$

it follows that $(0, \eta)$ is a tangential variation. By an argument used earlier in the proof of Lemma 4.1 we find $(\eta) \equiv (0)$. But the variation satisfies (9.12). Therefore by the condition of strong normality for the first set of conditions (9.4), $(\lambda) = 0$. This contradicts the independence of the solutions (9.10) and establishes the non-vanishing of (9.11). By taking appropriate linear combinations of the columns of the (9.11) we can obtain r linearly independent special accessory extremals

$$\alpha_{k\iota},\ \eta_{k\iota}(t) \qquad (k = 1,2,\ldots,r) \tag{9.13}$$

with $\alpha_{k\iota} = \delta_{k\iota}$, $\eta_{k\iota}(t_a) = y_{\iota ak}$, and multipliers $\lambda_{\tau k}$. Clearly these variations satisfy (6.4a) and (9.6).

Returning now to (9.5) we shall show that it is sufficient to prove the existence of a constant c such that (9.5) is positive for all linear combinations of (9.13) with $(\alpha) \not\equiv (0)$. In fact we shall prove that for every variation satisfying (6.4a) and (9.6) there is a linear combination of (9.13) with the same components (α) which gives I_2 a value not greater than that given by the original variation. It is convenient to introduce the following notation at this point. For any two admissible variations (α, η), $(\bar\alpha, \bar\eta)$ let

$$I_2(\alpha,\eta;\bar\alpha,\bar\eta) = g_{hk}\alpha_h\bar\alpha_k + \int_{t_1}^{t_2} (\omega_{\alpha_h}\bar\alpha_h + \omega_{\eta_i}\bar\eta_i + \omega_{\eta'_i}\bar\eta'_i)dt,$$

where the arguments in the derivatives of ω are (α, η, η'). It is easy to verify that $I_2(\alpha, \eta; \alpha, \eta) = I_2(\alpha, \eta)$, $I_2(\alpha, \eta; \bar\alpha, \bar\eta) = I_2(\bar\alpha, \bar\eta; \alpha, \eta)$, and I_2 is linear in each of its arguments (α, η) and $(\bar\alpha, \bar\eta)$. With this in mind let $(\bar\alpha, \bar\eta) \not\equiv (0, \bar\eta)$ be an admissible variation satisfying (9.6) and (6.4a). Let (α, η) be the linear combination $\bar\alpha_k\alpha_{k\iota}$, $\bar\alpha_k\eta_{k\iota}$ of the variations (9.13) and $\lambda_\tau = \alpha_k\lambda_{\tau k}$. The variation $(\bar\alpha - \alpha, \bar\eta - \eta)$ then has the form $(0, \eta^*)$ with $\eta^*_i(t_1) = \eta^*_i(t_2) = 0$, and satisfies both (9.6) and (9.7). Hence $I_2(0, \eta^*) \geqslant 0$ (see remark following (2.12)). We observe that

$$\begin{aligned} I_2(0,\eta^*) &= I_2(\bar\alpha - \alpha, \bar\eta - \eta; \bar\alpha - \alpha, \bar\eta - \eta) \\ &= I_2(\bar\alpha, \bar\eta) - 2I_2(\bar\alpha, \bar\eta; \alpha, \eta) + I_2(\alpha, \eta) \\ I_2(0,\eta^*; \alpha, \eta) &= I_2(\bar\alpha - \alpha, \bar\eta - \eta; \alpha, \eta) \\ &= I_2(\bar\alpha, \bar\eta; \alpha, \eta) - I_2(\alpha, \eta). \end{aligned} \tag{9.14}$$

But

$$I_2(0, \eta^*; a, \eta) = \int_{t_1}^{t_2} (\omega_{\eta_i} \eta_i^* + \omega_{\eta_i'} \eta_i'^*) dt$$

$$= \int_{t_1}^{t_2} (\omega_{\eta_i} \eta_i^* + \omega_{\eta' i} \eta_i'^*) dt + \lambda_\tau I_{\tau 1}(0, \eta^*)$$

$$= \int_{t_1}^{t_2} (\Omega_{\eta_i} \eta_i^* + \Omega_{\eta' i} \eta_i'^*) dt = [\Omega_{\eta' i} \eta_i^*]_{t_1}^{t_2} = 0.$$

Whence (9.14) yields $I_2(a, \eta) = I_2(\bar{a}, \bar{\eta}; a, \eta)$, and $I_2(0, \eta^*) = I_2(\bar{a}, \bar{\eta}) - I_2(a, \eta)$. Therefore $0 \leqslant I_2(\bar{a}, \bar{\eta}) - I_2(a, \eta)$, as desired.

Along the family of variations spanned by (9.13) the function I_2 is a quadratic form $Q(a)$ in the finite set of variables a_k. The function $Q(a)$ is positive for all $(a) \neq (0)$ such that $L_\sigma(a) = 0$. Our proof will be complete if we can show the existence of a constant c such that

$$Q(a) + cL_\sigma(a)_\sigma L(a) \tag{9.15}$$

is positive for all $(a) \neq (0)$. It is sufficient to restrict ourselves to the unit sphere

$$\sum_k a_k^2 = 1;$$

we are to understand that all point sets are taken relative to this space. The points satisfying $L_\sigma = 0$ form a closed set on which Q is positive. Hence there exists an open neighbourhood of this closed set on which Q is positive. On the complement of the neighbourhood $L_\sigma L_\sigma$ attains a positive minimum m, and $|Q|$ attains a maximum M. Let c be any number with $c > M/m$. Then c is the desired constant.

10. Further sufficient conditions for a relative minimum. For the statement of the next two theorems we shall need the following definition. A *normed element* (a, y, y') is one for which $y'_i y'_i = 1$. By a *neighbourhood* of the elements (a, y, y') on an admissible arc E we will now understand a set of elements (a, y, y') whose normed elements lie in a neighbourhood of the normed elements belonging to E. We shall say that an isoperimetric extremal E satisfies the Weierstrass condition II if it satisfies the Weierstrass condition II_N as defined in §6 with the modification that the elements (a, l, y, y') are restricted to belong to E. The next result deals with sufficient conditions for a weak relative minimum.

THEOREM 10.1. *If a non-singular isoperimetric extremal E_0 which does not intersect itself satisfies the conditions* (6.1), *the transversality condition, the Clebsch condition, and is such that the second variation of I along E_0 is positive, then there exists a neighbourhood $\mathfrak{N}_0$ in ayy'-space of the elements (a, y, y') belonging to E_0 such that $I(C) > I(E_0)$ for every admissible arc C in R_0 satisfying* (6.1) *but not identical with E_0.*

To prove the theorem we employ a standard result in the calculus of variations [3, pp. 110-111], which states that for a non-singular isoperimetric extremal E_0 satisfying the Clebsch condition there exists a neighbourhood $\mathfrak{N}_0$ and a neighbourhood $\mathfrak{L}$ such that $E[a, ly, y', Y'] > 0$ for (a, y, y') and (a, y, Y') in $\mathfrak{N}_0$, and (l) in $\mathfrak{L}$. Then for this region $\mathfrak{N}_0$ the arc E_0 satisfies the hypotheses of Theorem 6.1 and the theorem follows.

THEOREM 10.2 *Let the region $\mathfrak{R}$ of admissible elements consist of all sets (a, y, y') with (a, y) in an open set of ay-space and $y'_{\alpha'} \neq 0$. Then if a non-singular isoperimetric extremal E_0 which does not intersect itself satisfies the conditions* (6.1), *the transversality condition, the Weierstrass condition* II, *and is such that the second variation of I along E_0 is positive, then there exists a neighbourhood $\mathfrak{F}$ of E_0 in ay-space such that $I(C) > I(E_0)$ for every admissible arc C in $\mathfrak{F}$ satisfying* (6.1) *but not identical with E_0.*

The Weierstrass condition II and non-singularity imply that the Weierstrass and Clebsch conditions hold alone E_0 with the strict inequality sign [7]. These conditions in turn imply, for a region of the type described in the theorem, that the Weierstrass condition II_N holds [3, pp. 130-131]. Our theorem is then a consequence of Theorem 6.1.

REFERENCES

1. G. D. Birkhoff and M. R. Hestenes, *Natural isoperimetric conditions in the calculus of variations*, Duke Math. J., vol. 1 (1935), 198–286.
2. G. A. Bliss, *Normality and abnormality in the calculus of variations*, Trans. Amer. Math. Soc., vol. 43 (1938), 365–376.
3. ———, *Lectures on the calculus of variations* (Chicago, 1946).
4. M. R. Hestenes, *A note on the Jacobi condition for parametric problems in the calculus of variations*, Bull. Amer. Math. Soc., vol. 40 (1934), 297–302.
5. ———, *Generalized problem of Bolza in the calculus of variations*, Duke Math. J., vol. 5 (1939), 309–324.
6. ———, *Sufficient conditions for the isoperimetric problem of Bolza in the calculus of variations*, Trans. Amer. Math. Soc., vol. 60 (1946), 93–118.
7. M. R. Hestenes and W. T. Reid, *A note on the Weierstrass condition in the calculus of variations*, Bull. Amer. Math. Soc., vol. 45 (1939), 471–473.

The University of Chicago

THE INDEX OF AN EXTREMAL ARC

WILLIAM KARUSH

1. Introduction. We are concerned with extremal arcs for the problem of minimizing a function

$$I(C) = g(a) + \int_{t_1}^{t_2} f(a, y, y')dt \tag{1.1}$$

over a class of parametric curves C in ay-space of the form

$$a_h, \; y_i(t) \qquad (h = 1, 2, \ldots, r; \; i = 1, 2, \ldots, n; \; t_1 \leqslant t \leqslant t_2) \tag{1.2}$$

and satisfying end conditions of the type

$$y_i(t_s) = y_{is}(a) \qquad (s = 1, 2). \tag{1.3}$$

The components a_h are constants and the functions g, y_{is}, and f are given, with the last function positively homogeneous of degree one.

We propose to consider several definitions for the index of an extremal of this problem, and to show that under appropriate hypotheses these indices are equivalent.

The first index defined is the so-called index of the second variation I_2 of I. A second index is then formulated in terms of families of curves (1.2); this index is of interest because its definition does not make use of the second variation or of topological considerations. A third index, the isoperimetric index, is treated next; it is similar to that of Birkhoff and Hestenes [**1**] (see also [**2**]). It is then shown that these three indices are equal in the non-degenerate case. In the next section it is shown that these indices are equal to the index of a critical point for a certain function of a finite number of real variables, which is defined in terms of broken extremals. In the final section we treat the topological index. The definition is not the most general one but it serves to indicate the relationship with the other indices. (For a more complete treatment of topological critical curves see [**3**], [**5**], and [**7**].) We show under the additional assumptions of positive definiteness and positive regularity for I that the topological index is equal to the earlier indices.

The precise analytic formulation of the extremum problem treated here is given in a preceding paper by the author [**4**]. To save space, frequent references will be made to the definitions, formulae, and theorems of that paper.

Throughout the paper we shall assume that E denotes a *non-singular extremal which does not intersect itself and which satisfies the end conditions* (1.3) *and the transversality condition* [**4**, (2.8)].

2. Index of the second variation. We fix our attention upon a particular extremal E; the results below hold relative to this arc.

Received August 29, 1950.

In [4] we dealt with (admissible) variations a_h, η_i (a_h constant); we shall use simply η to designate such variations (a, η). In particular $\eta = 0$ is the variation $(a, \eta) = (0, 0)$. Let $\mathfrak{H}$ denote the linear class of variations (real scalars) which satisfy, along E, the accessory end conditions

$$\eta_i(t_s) = y_{ish}a_h \qquad (s = 1, 2). \tag{2.1}$$

(Here the first subscript "h" denotes differentiation with respect to a_h; also, a repeated index indicates summation over that index.)

The second variation of I along E is given by [4, (2.10)]; it is now designated by $I_2(\eta)$ instead of $I_2(a, \eta)$. Let $\mathfrak{H}'$ be a maximal linear subset of $\mathfrak{H}$ of finite dimension (possibly zero) on which I_2 is negative definite, i.e., for which $I_2(\eta) < 0$ for $\eta \neq 0$ in $\mathfrak{H}'$. The dimension k of $\mathfrak{H}'$ will be called the *index of* I_2 on $\mathfrak{H}$. If no such $\mathfrak{H}'$ of finite dimension exists, then we shall say that the index is infinite.

Associated with the second variation is the bilinear form

$$I_2(\eta, \bar{\eta}) = b_{hk}a_h\bar{a}_k + \int_{t_1}^{t_2}(\omega_{a_h}\bar{a}_k + \omega_{\eta_i}\bar{\eta}_i + \omega_{\eta'_i}\bar{\eta}'_i)dt, \tag{2.2}$$

where the arguments in the derivatives of ω are those belonging [4, (2.11)] to η. The function (2.2) is the first variation of $I_2(\eta)$. The following properties are obvious: (2.2) is linear in each of its arguments, it is symmetric in its arguments, and it reduces to the second variation for $\eta = \bar{\eta}$. We use I_2 to designate the second variation of I or (2.2); the context in every case will make the equation unambiguous.

A variation η in $\mathfrak{H}$ is *orthogonal* to a subset of $\mathfrak{H}$ in case $I_2(\eta, \bar{\eta}) = 0$ whenever the second argument belongs to the subset. A tangential variation (i.e., one of the form 0, $w(t)y_i(t)$ where y_i belongs to E) which belongs to $\mathfrak{H}$ is orthogonal to every variation; this follows from the homogeneity of f. One subset is orthogonal to another in case each variation of the first subset is orthogonal to each variation of the second.

The proofs below are phrased for finite-dimensional, linear subspaces. Where the complete proof requires extension to the infinite case, such extension will be obvious.

LEMMA 2.1. *The index k of I_2 on $\mathfrak{H}$ is uniquely defined.*

Let $\mathfrak{H}'$, $\mathfrak{H}''$ be maximal linear subsets of $\mathfrak{H}$ of finite dimension on which I_2 is negative definite with bases $\eta_1, \ldots, \eta_p$ and $\bar{\eta}_1, \ldots, \bar{\eta}_q$ respectively. (Subscripts here denote different vector functions, not separate components as in (2.2)). Suppose $p > q$. Then there exist constants c_i, not all zero, such that

$$I_2(\bar{\eta}_j, \eta_i)c_i = I_2(\bar{\eta}_j, \eta) = 0,$$

where $\eta = c_i\eta_i$. Hence η is orthogonal to $\mathfrak{H}''$. For any variation $\bar{\eta} + b\eta$ with b = constant, $\bar{\eta}$ in $\mathfrak{H}''$, and not both b and $\bar{\eta}$ zero,

$$I_2(\bar{\eta} + b\eta) = I_2(\bar{\eta}) + 2bI_2(\bar{\eta}, \eta) + b^2I_2(\eta) < 0.$$

It follows that $\mathfrak{H}''$ is not maximal. Hence $p \leqslant q$. Similarly, $q \leqslant p$. Therefore $p = q$, and the proof is complete.

Suppose $\mathfrak{H}$ contains a maximal linear subset $\mathfrak{H}_0$ of finite dimension which is orthogonal to $\mathfrak{H}$ and contains no non-zero tangential variation. Then the dimension d of $\mathfrak{H}_0$ will be called the *order of degeneracy* of I_2 on $\mathfrak{H}$. If no such subset exists the order of degeneracy will be said to be infinite. In case $d = 0$ the second variation I_2 will be called *non-degenerate on* $\mathfrak{H}$.

LEMMA 2.2. *The order of degeneracy d is uniquely defined.*

Let $\mathfrak{H}_0$, $\mathfrak{H}_1$, be maximal linear subsets of finite dimension which contain no non-zero tangential variation and are orthogonal to $\mathfrak{H}$. Suppose the dimension p of the first subset exceeds the dimension q of the second. Then at least one variation $\eta \neq 0$ of $\mathfrak{H}_0$ is not expressible as an element of $\mathfrak{H}_1$ plus a tangential variation (possibly 0). Then the subset with dimension $q + 1$ spanned by $\mathfrak{H}_1$ and η contains no non-tangential variation and is orthogonal to $\mathfrak{H}$, contrary to $\mathfrak{H}_1$ being maximal. Hence $p \leqslant q$. Similarly $q \leqslant p$, and thus $p = q$.

LEMMA 2.3 [cf. **1**; **2**]. *If E satisfies the Clebsch condition the integers k and d are finite.*

LEMMA 2.4. *Let $\mathfrak{H}'$ be a maximal linear subset of $\mathfrak{H}$ on which I_2 is negative definite. Let $\mathfrak{D}$ be the set of elements in $\mathfrak{H}$ which are orthogonal to $\mathfrak{H}'$. Then every element of $\mathfrak{H}$ can be written uniquely as the sum of an element of $\mathfrak{H}'$ and an element of $\mathfrak{D}$. Furthermore, $I_2(\eta) \geqslant 0$ for every η in $\mathfrak{D}$, the equality holding only in case η is orthogonal to the whole space $\mathfrak{H}$.*

Let $\bar{\eta}_1, \ldots, \bar{\eta}_k$ be a basis for $\mathfrak{H}'$ and η be an arbitrary element of $\mathfrak{H}$. Since the determinant $|I_2(\bar{\eta}_i, \bar{\eta}_j)|$ does not vanish we can select (c) such that

$$I_2(\eta, \bar{\eta}_j) = c_i I_2(\bar{\eta}_i, \bar{\eta}_j).$$

Hence $\eta - c_i\bar{\eta}_i$ is in $\mathfrak{D}$, and we have the decomposition $\eta = c_i\bar{\eta}_i + (\eta - c_i\bar{\eta}_i)$ To prove the uniqueness assume for the moment that the second conclusion of the theorem holds. Let

$$\eta = \eta_1 + \eta_2 = \eta^*_1 + \eta^*_2$$

with η_1, η^*_1 in $\mathfrak{H}'$ and η_2, η^*_2 in $\mathfrak{D}$. Then $\eta^*_2 - \eta_2 = \eta_1 - \eta^*_1$. Since the left member is in $\mathfrak{D}$ and the right member is in $\mathfrak{H}'$, we have

$$0 \leqslant I_2(\eta^*_2 - \eta_2) = I_2(\eta_1 - \eta^*_1) \leqslant 0.$$

Whence $\eta_1 = \eta^*_1$, $\eta_2 = \eta^*_2$ as desired. To establish the second half of the theorem suppose η were an element of $\mathfrak{D}$ with $I_2(\eta) < 0$. For b = constant and $\bar{\eta}$ in $\mathfrak{H}'$ we would have

$$I_2(\bar{\eta} + b\eta) = I_2(\bar{\eta}) + b^2 I_2(\eta) < 0,$$

unless $b = 0$, $\bar{\eta} = 0$, contrary to $\mathfrak{H}'$ being maximal. Finally, let $I_2(\eta) = 0$. Suppose there were an η^* in $\mathfrak{D}$ not orthogonal to η. Then

$$I_2(\eta^* + b\eta) = I_2(\eta^*) + 2bI_2(\eta^*, \eta) < 0,$$

for a suitable b. As just seen, this is a contradiction. Thus η is orthogonal to $\mathfrak{D}$, and since it is also in this subset it is orthogonal to $\mathfrak{H}'$. From the first part of the proof it follows that η is orthogonal to $\mathfrak{H}$, as desired.

LEMMA 2.5. *Let $\mathfrak{H}_1$ be a linear subset, containing no non-zero tangential variation, on which I_2 is non-positive. Then* dim $\mathfrak{H}_1 \leqslant k + d$. *The equality holds in case $\mathfrak{H}_1$ is maximal with these properties.*

Suppose dim $\mathfrak{H}_1 > k + d$. Select a subset $\mathfrak{H}^*_1$ of $\mathfrak{H}_1$ with finite dimension q greater than $k + d$, and let $\mathfrak{D}_1$ be the elements of $\mathfrak{H}^*_1$ which are orthogonal to $\mathfrak{H}$. Then $\mathfrak{H}^*_1$ has a basis in which the first d_1 elements form a basis for $\mathfrak{D}_1$ and the remaining elements span a subset which we shall denote by $\mathfrak{H}_2$. Since dim $\mathfrak{D}_1 \leqslant d$, we have dim $\mathfrak{H}_2 > k$. Following the device used in the proof of Lemma 2.1 we can choose an element $\eta \neq 0$ in $\mathfrak{H}_2$ which is orthogonal to $\mathfrak{H}'$ of Lemma 2.4. From that lemma, $I_2(\eta) \geqslant 0$. But $I_2(\eta) \leqslant 0$ since η is in $\mathfrak{H}_1$. Hence $I_2(\eta) = 0$, η is orthogonal to $\mathfrak{H}$ by the same lemma, and η belongs to $\mathfrak{D}_1$. This implies that $\mathfrak{H}_2$ and $\mathfrak{D}_1$ have a non-zero element in common, which contradicts the definition of $\mathfrak{H}_2$. Inasmuch as we shall not make use of the second part of the lemma we shall not pause to prove it.

3. Index of an extremal. In this section we propose a definition of index without resort to the second variation or to topological methods.

Let $\mathfrak{E}$ be the class of admissible arcs a_h, $y_i(t)$ which satisfy the end conditions (1.3). Consider a q-parameter family of arcs

$$a_h = a_h(b_1, \ldots, b_q), \quad y_i = y_i(t, b_1, \ldots, b_q) \qquad (t_1 \leqslant t \leqslant t_2, \quad h = 1, 2, \ldots, r; \quad i = 1, 2, \ldots, n) \tag{3.1}$$

in $\mathfrak{E}$ which contains E for $(b) = (0)$. For (t, b), near the values belonging to E, the functions in (3.1) are supposed to have continuous first and second derivatives relative to the components of (b), and these derivatives, in turn, are to have piecewise continuous derivatives relative to t. The family is said to be of dimension q on E if the variations

$$\eta_p\colon \quad a_{hb_p}(0), \quad y_{ib_p}(t, 0) \qquad (p = 1, 2, \ldots, q) \tag{3.2}$$

span a linear space of dimension q which contains no non-zero tangential variation. Along (3.1) the integral I defines a function $I(b)$. By the *index m of E on $\mathfrak{E}$* will be meant the least upper bound of the integers q for which there exists a family (3.1) of dimension q on E such that the corresponding function $I(b)$ has a proper relative maximum at $(b) = (0)$.

THEOREM 3.1. *The index m of E on $\mathfrak{E}$ satisfies the inequality $k \leqslant m \leqslant k + d$ where k is the index of I_2 on $\mathfrak{H}$ and d in the order of degeneracy of I_2 on $\mathfrak{H}$. If I_2 is non-degenerate on $\mathfrak{H}$ then $m = k$.*

Let $\eta_1, \ldots, \eta_k$ be the basis of a linear subset $\mathfrak{H}'$ as in Lemma 2.4. Let $a_{k0}, y_{i0}(t)$ define E and let

$$a_k(b) = a_{k0} + a_{kp}b_p, \quad Y_i(t, b) = y_{i0}(t) + \eta_{ip}(t)b_p \qquad (p = 1, 2, \ldots, k).$$

Then the k-parameter family

$$a_k(b), \quad y_i(t, b) = Y_i(t, b) + h_{i1}(b)(t_2 - t) + h_{i2}(b)(t - t_1)$$

where

$$h_{is}(b) = \frac{y_{is}(a(b)) - Y_i(t_s, b)}{t_2 - t_1} \qquad (s = 1, 2),$$

lies in $\mathfrak{E}$ and has η_p as its variations (3.2). Hence the family has dimension k. The function $I(b)$ has at $(b) = (0)$ the differentials

$$dI = I_1(\delta y), \quad d^2I = I_2(\delta y)$$

where δy is $\eta_p db_p$. Since E is an extremal satisfying the transversality condition, $dI = 0$. Furthermore $d^2I < 0$ for all $(db) \neq (0)$. Thus $I(b)$ has a proper relative maximum at $(b) = (0)$, and $k \leqslant m$. To prove $m \leqslant k + d$ let (3.1) define a family of dimension q for which $I(b)$ has a proper relative maximum at $(b) = (0)$. It follows that

$$dI(0) = I_1(\delta y) = 0, \quad d^2I(0) = I_2(\delta y) \leqslant 0,$$

with δy as above and variations (3.2). The linear subset spanned by (3.2) satisfies the hypotheses of Lemma 2.5. Hence $q \leqslant k + d$, $m \leqslant k + d$, as desired.

4. **Isoperimetric index.** Consider a set of q isoperimetric conditions

$$I_p(C) = g_p(a) + \int_{t_1}^{t_2} f_p(a, y, y')dt = 0 \qquad (p = 1, 2, \ldots, q) \tag{4.1}$$

for which the arc E is normal, i.e., there is no linear combination $c_pI_p(c) \neq (0)$ for which E is an extremal satisfying the transversality condition. By the *isoperimetric index* k' of E will be meant the least of the integers q for which there exist conditions (4.1) such that E affords I a weak relative minimum in the class of admissible arcs C satisfying (1.3) and (4.1). If no such finite (possibly 0) integer q exists the isoperimetric index will be said to be infinite. The idea of defining index by the adjunction of isoperimetric conditions was used by Birkhoff and Hestenes in [1] where they employed "natural" isoperimetric conditions.

LEMMA 4.1. *For any variation $\bar{\eta}$: $\bar{a}_k$, $\bar{\eta}_i(t)$ in $\mathfrak{H}$ of class C''' there exists a set of functions $\xi_i(a, y)$ defined and of class C''' in a neighbourhood of the values (a, y) belonging to E such that along E we have $\xi_i(a_0, y_0(t)) = \bar{\eta}_i(t)$ and such that the first variation of the function*

$$I_1(\xi; C) = g_k\bar{a}_k + \int_C (f_{a_k}\bar{a}_k + f_{y_i}\xi_i + f_{y'_i}\xi_{iy'_j}y'_j)dt \tag{4.2}$$

has the form $I_2(\bar{\eta}, \eta)$ along E for η in $\mathfrak{H}$.

We show first the existence of functions ξ_i for which the first equation in the conclusion holds and such that

$$\xi_i(a, y_s(a)) = y_{isk}(a)\bar{a}_k. \tag{4.3}$$

Assume $(\bar{a}) \neq 0$; say the first component does not vanish. Select $r - 1$ variations η_k: $a_{hk}, \eta_{ik}(t)$ $(k = 2, 3, \ldots, r)$ in $\mathfrak{H}$ of class C''' for which

$$a_{hk} = \delta_{hk} \tag{4.4}$$

where the symbol on the right is the Kronecker delta. Since the variations satisfy (2.1),

$$\eta_{ik}(t_s) = y_{isk}(a_0). \tag{4.5}$$

Now if we define η_{i1} by

$$\bar{a}_1\eta_{i1} + \bar{a}_2\eta_{i2} + \ldots + \bar{a}_r\eta_{ir} = \bar{\eta}(t) \tag{4.6}$$

and select a_{h1} to satisfy (4.4), then equations (4.4) and (4.5) hold for $k = 1, 2, \ldots, r$.

Next, define the family $a_h, y_i(t, a)$ as in [4, (3.4)]. Then

$$y_i(t_s, a) = y_{is}(a), \quad y_{ia_h}(t, a_0) = \eta_{ih}(t). \tag{4.7}$$

Choose functions $u_{ij}(t)$ $(j = 1, 2, \ldots, n - 1)$ of class C''' such that the determinant $|y'_{i0}\, u_{ij}|$ does not vanish on t_1t_2. Then the equations $y_i = y_i(t, a) + u_{ij}(t)e_j$ have initial solutions (a, y, t, e) for values (a, y, t) belonging to E and $(e) = (0)$, the functional determinant with respect to (t, e) does not vanish on t_1t_2, and no two distinct points (a, y, t, e) have the same projection (a, y) since E does not intersect itself. Hence there exist unique solutions $t = t(a, y), e_j = e_j(a, y)$ of these equations defined and of class C''' in a neighbourhood of the values (a, y) belonging to E. Furthermore, the solutions satisfy

$$t(a_0, y_0(t)) = t, \quad t(a, y_s(a)) = t_s \qquad (s = 1, 2). \tag{4.8}$$

Define

$$\eta_i(a, t) = y_{ia_h}(t, a)\bar{a}_h.$$

Then the desired functions are $\xi_i(a, y) = \eta_i(a, t(a, y))$. For, from equations (4.6), (4.7), and (4.8),

$$\xi_i(a_0, y_0(t)) = \eta_i(a_0, t) = y_{ia_h}(t, a_0)\bar{a}_h = \eta_{ih}(t)\bar{a}_h = \bar{\eta}_i(t),$$

$$\xi_i(a, y_s(a)) = \eta_i(a, t_s) = y_{ia_h}(t_s, a)\bar{a}_h = y_{ish}(a)\bar{a}_h.$$

Now suppose $(\bar{a}) = (0)$. In this case we select r arbitrary variations satisfying (4.4) and (4.5) and determine $t(a, y)$ as above. Then the desired functions are $\xi_i(a, y) = \bar{\eta}_i(t(a, y))$.

It remains to calculate the first variation of (4.2) along E. We find it to be

$$g_{hk}\bar{a}_h a_k + \int_{t_1}^{t_2}\left(f_{y_i}\delta\xi_i + f_{y'_i}\frac{d}{dt}\delta\xi_i\right)dt + \int_{t_1}^{t_2}(\omega_{a_h}\bar{a}_h + \omega_{\eta_i}\bar{\eta}_i + \omega_{\eta'_i}\bar{\eta}'_i)dt,$$

where

$$\delta\xi_i = \xi_{i\alpha_k}a_k + \xi_{iy_j}\eta_j,$$

evaluated at E. Using (2.1) and the result of differentiating (4.3) we find the second term above to equal

$$\int_{t_1}^{t_2}\frac{d}{dt}(f_{y'_i}\delta\xi_i)dt = [f_{y'_i}\delta\xi_i]_{t_1}^{t_2} = [f_{y'_i}(\xi_{i\alpha_k}a_k + \xi_{iy_j}y_{j\alpha_k}a_k)]_{t_1}^{t_2} = [f_{y'_i}y_{i\alpha_k}\bar{a}_k a_k]_{t_1}^{t_2}.$$

The theorem follows from (2.2) and [4, (2.11)].

THEOREM 4.1. *Let E be a non-singular extremal for the function I which does not intersect itself and satisfies the end conditions* (1.3) *and the transversality condition. Suppose that E satisfies the Clebsch condition and that the second variation I_2 of I along E is non-degenerate. Then the isoperimetric index k', the index m of E, and the index k of the second variation of I along E are all finite and equal.*

Lemma 2.3 establishes the finiteness of k, and Theorem 3.1 the equality $m = k$. We shall show $k = k'$. Select a maximal linear subspace $\mathfrak{H}'$ as in Lemma 2.4. By appropriate modification of a basis of $\mathfrak{H}'$ we obtain another subspace $\mathfrak{H}'$ for which each element of its basis is of class C'''. Consider such a subspace. For each η_q construct the function ξ_q of Lemma 4.1. Consider the isoperimetric conditions

$$I_1(\xi_q; C) = 0 \qquad (q = 1, 2, \ldots, k) \tag{4.9}$$

determined by (4.2). We now make use of the sufficiency theorem [4, Theorem 10.1]. We note first that E satisfies (4.9), since along E the left side of (4.9) is the first variation of I evaluated at η_q. The arc E with multipliers $l_q = 0$ will satisfy the conditions of the above-mentioned sufficiency theorem for the problem of minimizing I relative to the end conditions (1.3) and the isoperimetric conditions (4.9) if we show the following: that the second variation I_2 of I along E is positive for non-tangential variations in $\mathfrak{H}$ which make the first variation of each function on the left in (4.9) vanish. By Lemma 4.1, the condition that the first variation vanish is $I_2(\eta_q, \eta) = 0$, that is, orthogonality to $\mathfrak{H}'$. By Lemma 2.4, for such an orthogonal variation $I_2(\eta) \geqslant 0$, the equality holding just in case η is orthogonal to $\mathfrak{H}$. From the non-degeneracy of I_2 the only non-zero variations orthogonal to $\mathfrak{H}$ are the tangential variations. From this the desired condition on I_2 is verified and we may deduce that $I(E)$ is a weak relative minimum relative to (1.3) and (4.9). Also, E is normal relative to (4.9); for otherwise E would be an extremal satisfying the transversality condition for a function which is a linear combination of the left sides of (4.9) with coefficients $(c) \neq (0)$. Thus the first variation $c_q I_2(\eta_q, \eta)$ of this function would vanish for all η in $\mathfrak{H}$, contrary to the assumption of non-degeneracy. We may conclude that $k' \leqslant k$.

To show the reverse inequality, consider a set of isoperimetric conditions $I_p(C) = 0$ $(p = 1, 2, \ldots, k')$ for which E is normal and such that $I(E)$ is a weak relative minimum relative to these conditions and (1.3). Then a necessary condition on E is $I_2(\eta) \geqslant 0$ for η in $\mathfrak{H}$ satisfying the first variation conditions

$I_{p1}(\eta) = 0$. Suppose $k' < k$. Let $\eta_1, \ldots, \eta_k$ be a basis for $\mathfrak{H}'$ as in Lemma 2.4. There exist coefficients $(c) \neq (0)$ such that $c_q I_{p1}(\eta_q) = I_{p1}(\eta) = 0$, where $\eta = c_q \eta_q \neq 0$. Thus $I_2(\eta) > 0$, contrary to η being in $\mathfrak{H}'$. Thus $k \leqslant k'$, $k = k'$, and the proof is complete.

5. Additional results. Let $f(z)$ be a function of a finite number of variables $(z_1, \ldots, z_m)$ which is of class C'' in the neighbourhood of a point $(z) = (z_0)$. We shall say that $(z) = (z_0)$ is an *analytical critical point of index k* in case at (z_0) we have (i),

$$f_{z_j} = 0 \qquad (j = 1, \ldots, m),$$

and (ii), the quadratic form

$$f_{z_i z_j} dz_i dz_j$$

has negative index k. An analytical critical point will be called *non-degenerate* in case the Hessian

$$|f_{z_i z_j}|$$

does not vanish there. It is well known that the index of a non-degenerate critical point (z_0) is equal to the dimension of a maximal linear subspace of (dz)-space on which the quadratic form

$$f_{z_i z_j} dz_i dz_j$$

is negative definite.

We wish to make use of certain results in the proof of [4, Theorem 8.1]. These results depend upon the assumptions on E made in the last paragraph of §1 and, in addition, the hypothesis that E satisfies the Weierstrass condition Π_N. (Not all the hypotheses of [4, Theorem 8.1] are required for the results we shall use.) Instead of this Weierstrass condition we shall assume the Clebsch condition on E. This will only change the extremum properties in [4] from those of strong relative minima to those of weak relative minima. We may see this as follows. Let $\mathfrak{R}$ be the set of admissible points (a, y, y') for which the original problem of §1 is defined. From non-singularity and the Clebsch condition we deduce the existence of a neighbourhood $\mathfrak{R}_0$ of the values of (a, y, y') belonging to E for which E satisfies Π_N (see first statement in the proof of [4, Theorem 10.1]). Then the results we shall carry over from [4] are valid when $\mathfrak{R}$ is replaced by $\mathfrak{R}_0$, i.e., when in the original problem we replace strong minima by weak minima.

We now make use of the family of broken extremals

$$a_h, y_i = y_i(t, a, e) \tag{5.1}$$

given by [4, (8.9)]. (The variables (l) do not appear since there are no isoperimetric conditions.) This family contains the given arc E for values (a_0, e_0), and the extremal segments of these curves have the (weak) minimizing property described in [4, Theorem 7.2]. The variations

$$\bar{\eta}: \quad a_h = da_h, \quad \eta_i = y_{ia_h} da_h + y_{ie_r} de_r \tag{5.2}$$

of (5.1) form a linear space of broken special accessory extremals satisfying (2.1) and containing no tangential variation for $(da, de) \neq (0, 0)$. This space, call it $\mathfrak{H}_1$, is a subspace of $\mathfrak{H}$. (For the properties of (5.1) and (5.2) see [4, Theorem 7.2] and the proof of [4, Theorem 8.1].)

LEMMA 5.1. *Let k be the index of I_2. Then there exists a linear subset $\mathfrak{H}'_1$ of $\mathfrak{H}_1$ which is of dimension k and on which I_2 is negative definite.*

We shall show that for an arbitrary admissible variation η: $\mathfrak{a}_h$, η_i in $\mathfrak{H}$ there exists a variation $\bar{\eta}$ in $\mathfrak{H}_1$ with the same components $(\mathfrak{a})$ such that $I_2(\bar{\eta}) \leqslant I_2(\eta)$. It is clear from [4, (8.13)] that we can determine constants (da, de) and a function $w(t)$ of class C'' which vanishes at the end points such that

$$\eta_i(s_j) = \bar{\eta}_i(s_j) + w(s_j)y'_{i0}(s_j) \qquad (j = 1, 2, \ldots, q),$$

where $\bar{\eta}$ is given by (5.2) with $(da) = (\mathfrak{a})$. Let η^* represent the tangential variation $(0, wy'_0)$ and $\eta_0 = \eta - (\bar{\eta} + \eta^*)$. Then η_0 vanishes at the corner points s_j. Furthermore, since each segment of E between corner points affords I a weak relative minimum relative to admissible arcs joining its end points we must have $I_2(\eta_0) \geqslant 0$. Now

$$I_2(\eta_0) = I_2(\eta) - 2I_2(\eta, \bar{\eta} + \eta^*) + I_2(\bar{\eta} + \eta^*).$$

Using, in particular, the property that η^* and $\bar{\eta}$ satisfy the accessory Euler equations, we find that

$$I_2(\eta, \bar{\eta} + \eta^*) = I_2(\bar{\eta} + \eta^*) + I_2(\eta_0, \bar{\eta} + \eta^*) = I_2(\bar{\eta} + \eta^*),$$

$$I_2(\bar{\eta} + \eta^*) = I_2(\bar{\eta}) + 2I_2(\bar{\eta}, \eta^*) + I_2(\eta^*) = I_2(\bar{\eta}).$$

Hence $I_2(\eta_0) = I_2(\eta) - I_2(\bar{\eta})$, $I_2(\bar{\eta}) \leqslant I_2(\eta)$. Now let $\eta_1, \ldots, \eta_k$ be a basis of a linear subset $\mathfrak{H}'$ as in Lemma 2.4. For each η_p determine the variation $\bar{\eta}_p$ as above. If $\eta = c_p\eta_p$ is an arbitrary element of $\mathfrak{H}'$ the associated variation $\bar{\eta}$ determined above is $c_p\bar{\eta}_p$. Hence the linear subset spanned by $\bar{\eta}_p$ will satisfy the conclusion of the lemma.

THEOREM 5.1. *Let E satisfy the hypotheses of Theorem* 4.1. *Then the function $I(a, e)$ obtained by evaluating I along* (5.1) *has a non-degenerate analytical critical point at $(a, e) = (a_0, e_0)$ of index k if and only if the extremal E has index k.*

By Theorem 4.1 the index of E equals the index of I_2. For the function $I(a, e)$ we have, at (a_0, e_0), $dI = I_1(\bar{\eta})$, $d^2I = I_2(\bar{\eta})$ where $\bar{\eta}$ is given by (5.2). Suppose that (a_0, e_0) is a non-degenerate analytical critical point of index k_0. To a maximal linear subspace of (da, de)-space on which d^2I is negative definite there corresponds, through (5.2), a linear subset of $\mathfrak{H}$ of dimension k_0 on which I_2 is negative definite. Hence $k_0 \leqslant k$. Also, to the subset $\mathfrak{H}'_1$ of Lemma 5.1 there corresponds a linear subset in (da, de)-space of dimension k on which d^2I is negative definite. Hence $k \leqslant k_0$, $k = k_0$. Conversely, let E be an extremal of index k. Since the first variation of I vanishes at $\bar{\eta}$, the function $I(a, e)$ has an analytical critical point at (a_0, e_0). To prove non-degeneracy suppose that the

Hessian of $I(a, e)$ vanished there. There would exist constants $(da, de) \neq (0, 0)$ such that the corresponding non-tangential variation $\bar{\eta}$ of $\mathfrak{H}_1$ would be orthogonal to $\mathfrak{H}_1$. Since the latter set contains $\mathfrak{H}'_1$ of Lemma 5.1, by Lemma 2.4, $I_2(\bar{\eta}) > 0$. From the non-degeneracy of I_2 the equality sign could not hold. This is contrary to the fact that $\bar{\eta}$ is orthogonal to itself. Finally, the proof of the equality $k_0 = k$ is a repetition of the first part of the proof.

THEOREM 5.2. *Let the domain $\mathfrak{R}$ of elements (a, y, y') for which the extremum problem of §1 is defined consist of elements with (a, y) in an open set in ay-space and $y'_{\alpha}y'_{\epsilon} \neq 0$. In Theorem 4.1 replace the Clebsch condition by the Weierstrass condition* II. *The modified theorem is valid even if in the definition of isoperimetric index it is required that $I(E)$ be a strong, rather than weak, relative minimum.*

(See [4, §10] for the definition of condition II.) The proof is identical to that of Theorem 4.1 except for the use of [4, Theorem 10.2] instead of [4, Theorem 10.1].

We conclude the section with a method, based on Lemma 4.1, for constructing abnormal isoperimetric problems.

THEOREM 5.3. *Let η_p $(p = 1, 2, \ldots, q)$ be admissible variations of class C''' which satisfy* (2.1). *Suppose there exist constants c_p not all zero such that $\eta = c_p \eta_p$ is an accessory extremal satisfying the transversality condition for the second variation. Then the extremal E is abnormal relative to the isoperimetric conditions*

$$I_1(\xi_p; C) = 0 \qquad (p = 1, 2, \ldots, q), \tag{5.3}$$

where the functions appearing in (5.3) *are defined in Lemma* 4.1.

The condition of abnormality in this case is the existence of $(c) \neq 0$ such that

$$c_p\left(\omega_{\eta_i p} - \frac{d}{dt}\omega_{\eta' i p}\right) = 0,$$

$$c_p\left(b_{hk}a_{hp} + [\omega_{\eta' i p}y_{ih}]_1^2 + \int_{t_1}^{t_2}\omega_{\alpha_i p}dt\right) = 0.$$

(See [4, (8.1)]. Here $\omega_{\eta_i p}$ means ω_{η_i} evaluated at the variation η_p, etc.) The first condition is that η be an accessory extremal, and the second that this variation satisfy the transversality condition for I_2. The conclusion now follows [4, §8].

COROLLARY. *If in Theorem* 5.3 *we do not require η to satisfy the accessory transversality condition then the conclusion holds with "abnormal" replaced by "not strongly normal."*

6. Topological critical curves. In this section we shall assume a knowledge of modular Vietoris cycles on a metric space.

Let S be a metric space whose elements we denote by C. Let I be a real single-valued function on S and $\mathfrak{K}$ be the class of subsets K of S determined by $I \leqslant c$ for c real or $+\infty$. In the sequel K, K', etc., will denote members of $\mathfrak{K}$. Suppose that all the sets K for $c \neq \infty$ are compact. Consider a particular point C_0 of S

and let K denote the fixed set determined by $c = I(C_0)$. Then we shall say that C_0 is an *isolated topological critical point of index k and count* 1 in case:

(1) There exists a Vietoris k-cycle u on K mod K' such that $u \sim 0$ on K mod $(K - C_0)$, and if N is a neighbourhood of C_0 then there is a set $K'' \subset K$ such that $u \sim 0$ on K mod $(K'' + KN)$.

(2) If V is a k-cycle on K mod K_0 with property (1), then there exists a set $K'_0 \subset K$ such that $u \sim v$ on K mod K'_0. (Here $\subset$ denotes strict inclusion.)

Clearly C_0 is a critical point of index k and count 1 relative to the space S if and only if it is a similar critical point relative to the space K. The above definition of a critical point is not the most general one but it will serve our purpose of relating the topological index to the indices defined earlier. The definition here given was suggested by [3].

A homotopy Δ of a subset P of S into a subset Q of S is called an *I-deformation* in case I never increases under Δ, that is, if $h(C, t)$ (C on P, t on $0 \leqslant t \leqslant 1$) is the function defining Δ and $C' = h(C, t_1)$, then $I(C'') \leqslant I(C')$ for every $C'' = h(C, t)$ with $t_1 \leqslant t \leqslant 1$. For C in P, let $\Delta C = h(C, 1)$. Let ΔP be the set of points ΔC with C in P.

THEOREM 6.1. *Let C_0 be an isolated topological critical point of index k and count* 1. *Let N be a neighbourhood of C_0 and Δ be an I-deformation of N. Then C is a fixed point under Δ.*

Suppose that C_0 is not a fixed point. Then there exists a neighbourhood $N_0 \subseteq N$ of C_0 and an I-deformation Δ_1 such that $\Delta_1(KN_0) \subseteq (K - C_0)$. Let u be a modular k-cycle related to C_0 as in the definition of a critical point. From the second part of (1) of this definition we can assume that u is on KN_0. It follows that under Δ_1 the k-cycle u is deformed into a k-cycle on $(K - C_0)$. Hence $u \sim 0$ on K mod $(K - C_0)$, contrary to our choice of u. This proves the theorem.

We return now to the function $I(C)$ given by (1.1). In this section we shall make the following additional assumptions on I: (1) The region of admissible points (a, y, y') has the form (a, y) in a region $\mathfrak{R}$ of ay-space and $(y') \neq (0)$ arbitrary. (2) *Positive definiteness*, that is, the integrand function f is positive everywhere. (3) *Positive regularity*, that is, for each admissible element (a, y, y'),

$$f_{y'_i y'_j \sigma_i \sigma_j} > 0, \qquad (\sigma) \neq (ky').$$

We fix attention on a particular admissible curve E in $\mathfrak{R}$ satisfying the conditions stated at the end of §1. (Notice that positive regularity of I automatically ensures non-singularity and the Clebsch condition for E.) Let $\mathfrak{R}'$ be a neighbourhood of E such that the closure $\bar{\mathfrak{R}}'$ is contained in $\mathfrak{R}$. Let R be the class of all rectifiable curves in $\bar{\mathfrak{R}}'$ which satisfy (1.3). We introduce the usual Frechet metric in R. By standard theory, our hypotheses imply that the subsets of R determined by inequalities $(I(C) \leqslant c, c \neq \infty)$, are compact. We now make the following definition. The arc E is an *isolated topological critical curve of index k*

and count 1 in case there exists a closed Fréchet neighbourhood $S \subset R$ of E such that E is a critical point according to the earlier definition in the space S. Such a curve will be called simply a "critical curve." Let K be the compact subset of R determined by $I(C) \leqslant I(E)$. From the remark following the definition of critical point, we see that we can limit ourselves to the space K. Henceforth we shall do so and consider only subsets and neighbourhoods relative to K.

It is well known that under our hypotheses on the function I there exists a number $c > 0$ such that any two points in $\mathfrak{N}'$ within e-distance of each other can be joined in either direction by a unique extremal in $\mathfrak{N}$ which affords I a proper minimum relative to arcs in $\mathfrak{N}'$ joining its end points. These short minimizing extremals vary continuously with their end points, and I is continuous on this class of arcs. Pick a neighbourhood $\mathfrak{N}_0$ of E such that the short minimizing arcs with end points in $\mathfrak{N}_0$ all lie in $\mathfrak{N}'$.

Let

$$a_h(C), \quad y_i(t, C) \qquad (0 \leqslant t \leqslant 1, \quad C \text{ in } K) \tag{6.1}$$

be the special parameterization of curves given by Morse [6]. For each C in K the functions (6.1) define a parameterization of C, and the functions (6.1) are continuous in t and C simultaneously. From the compactness of K, there exists a number $d > 0$ such that if $|t_1 - t_2| \leqslant d$ and C is in K then the points given by (6.1) for $t = t_1$, and $t = t_2$ are within e-distance of each other. Let S be a closed Frechet neighbourhood of E such that all the curves of S lie in $\mathfrak{N}_0$. Let t_1t_2 be a sub-interval of $0 \leqslant t \leqslant 1$ of length less than d. We shall describe an I-deformation $\Delta(t_1, t_2)$ of S. Let C be any curve of S. When $t = 0$, leave C unaltered, when $0 < \tau \leqslant 1$ replace the sub-arc of C between t_1 and $t_1 + \tau(t_2 - t_1)$ by the short minimizing extremal joining its end points and directed in the same sense as C. By performing this deformation simultaneously on all the curves of S we obtain $\Delta(t_1, t_2)$.

THEOREM 6.2. *A critical curve is an extremal.*

For, by the deformation $\Delta(t_1, t_2)$ and Theorem 6.1 every sufficiently short sub-arc of E is an extremal. Therefore E itself is an extremal.

We wish now to show the equivalence of the topological index with the earlier indices. For this purpose we make the following construction. Subdivide the interval $0 \leqslant t \leqslant 1$ by points $t_0 = 0, t_1, \ldots, t_q, t_{q+1} = 1$ so that (1) the length of each sub-interval is less than d, (2) the arc E has on it no pairs of conjugate points between t_j and t_{j+1}, and (3) the length of arc on E between t_j and t_{j+1} is less than $e/6$. Let

$$(a_0, y_1(a_0)), \quad (a_0, b_{10}), \ldots, (a_0, b_{q0}), \quad (a_0, y_2(a_0))$$

be the points of subdivision on E. For nearby values (a, b) we can obtain a broken extremal with end and corner points given by the preceding sequence with the subscript zero deleted. In this way we obtain a family

$$a_h, \quad y_i(t, a, b) \tag{6.2}$$

of broken extremals with the continuity properties of the family [4, (8.7)]. Let $\mathfrak{B}$ be a neighbourhood of (a_0, b_0) such that for (a, b) in $\mathfrak{B}$ the arc (6.2) lies in $\mathfrak{N}$, has the length of each sub-arc between corners less than $e/3$, and intersects π_j once and only once. (Here π_0 and π_{q+1} are the end manifolds of (1.3) and $\pi_1, \ldots, \pi_q$ are $(n-1)$-dimensional hyperplanes through $(a_0, b_{10}), \ldots, (a_0, b_{q0})$ orthogonal to E.)

Apply the above subdivision of the interval $0 \leqslant t \leqslant 1$ to each of the curves (6.1), and let S be a closed Fréchet neighbourhood of E such that each curve of S is in $\mathfrak{N}_0$ and has its values (a, b) corresponding to the points of subdivision of the interval in the neighbourhood $\mathfrak{B}$. Let Δ be the I-deformation obtained by applying

$$\Delta\,(t_j, t_{j+1}) \qquad (j = 0, 1, \ldots, q)$$

simultaneously for all j. The homotopy Δ deforms S into the family (6.2). Our next step is to I-deform (6.2) into its sub-family having its corners on the hyperplanes π_j. To this end let

$$a_h = a_h, \quad y_i = b_i(e_{1,j}, e_{2,j}, \ldots, e_{n-1,j}) \qquad (j = 1, 2, \ldots, q)$$

be the equations of the hyperplanes π_j, where $b_i(e_{j0}) = b_{ij0}$. Then the sub-family is

$$a_h, \quad y_i(t, a, e) \equiv y_i[t, a, b(e)]. \tag{6.3}$$

Let C be an arc of the family (6.2) and denote its corner points by $P_1, P_2, \ldots, P_q$. Let $Q_1, Q_2, \ldots, Q_q$ be the points of intersection of C with $\pi_1, \pi_2, \ldots, \pi_q$. For any time τ on the interval $0 \leqslant \tau \leqslant 1$ let R_j $(j = 1, 2, \ldots, q)$ be the point of the sub-arc of C between P_j and Q_j such that the ratio of the distance P_jR_j (j not summed) along C to the distance P_jQ_j along C equals τ. Let R_0, R_{q+1} be the fixed end points of C. For all $j = 0, 1, \ldots, q$, replace the sub-arc of C between R_j and R_{j+1} by the short minimizing arc joining these points and directed in the same sense as C. As τ varies this construction when applied to all the curves (6.2) yields an I-deformation Δ' into (6.3). The product $\Delta'\Delta$ is an I-deformation of S into (6.3). From the invariance of homology relations under homotopy and from the fact that $\Delta'\Delta$ is an I-deformation we infer the following result:

THEOREM 6.3. *Let E be an extremal which does not intersect itself and satisfies the end conditions* (1.3). *Then E is an isolated topological critical curve of index k and count* 1 *if and only if (a_0, e_0) is an isolated topological critical point of index k and count* 1 *of the function $I(a, e)$, where $I(a, e)$ is the value of the integral I along the family* (6.3).

Now it is known that (a_0, e_0) is an isolated topological critical point of index k and count 1 for $I(a, e)$ if and only if the point is a non-degenerate analytical critical point of $I(a, e)$ of index k. The results of §5 for the family (5.1) are valid for the family (6.3). Thus, from Theorems 6.3 and 5.1 we obtain the following result:

THEOREM 6.4. *Under the assumptions of this section and Theorem* 5.1 *an extremal E is an isolated topological critical curve of index k and count* 1 *if and only if it is an extremal of index k.*

REFERENCES

1. G. D. Birkhoff and M. R. Hestenes, *Natural isoperimetric conditions in the calculus of variations*, Duke Math. J., vol. 1 (1935), 198-286.
2. K. E. Hazard, *Index theorems for the problem of Bolza*, Contributions to the Calculus of Variations, 1938-41 (Chicago).
3. M. R. Hestenes, *A theory of critical points*, Amer. J. Math., vol. 67 (1945), 521-562.
4. W. Karush, *Isoperimetric problems in the calculus of variations*, Can. J. Math., vol. 4 (1952), 257-280.
5. M. Morse, *The calculus of variations in the large* (American Mathematical Society, Colloquium Publications, vol. 18, 1934).
6. ———, *A special parameterization of curves*, Bull. Amer. Math. Soc., vol. 42 (1936), 915-922.
7. ———, *Functional topology and abstract variational theory*, Ann. Math., vol. 38 (1937), 386-449.

The University of Chicago

CYCLIC AFFINE PLANES

A. J. HOFFMAN

1. Introduction. Let Π be an affine plane which admits a collineation τ such that the cyclic group generated by τ leaves one point (say X) fixed, and is transitive on the set of all other points of Π. Such "cyclic affine planes" have been previously studied, especially in India, and the principal result relevant to the present discussion is the following theorem of Bose [2]: every finite Desarguesian affine plane is cyclic. The converse seems quite likely true, but no proof exists. In what follows, we shall prove several properties of cyclic affine planes which will imply that for an infinite number of values of n there is no such plane with n points on a line. Our results are approximately parallel to those obtained by Hall [6] in his investigation of cyclic projective planes (projective planes admitting a collineation τ such that the group generated by τ is transitive on *all* the points), and our methods are derived from his stimulating and penetrating work. One contrast with the projective case, however, is that every cyclic plane is necessarily finite; for if P and Q are points collinear with X, and if $Q = \tau^d P$, then τ^d leaves the line $P\,Q\,X$ fixed, which implies that the orbit of P under τ belongs to a finite set of lines, and hence cannot contain all points of an infinite plane.

2. Affine difference sets. The integer n will always be the number of points on a line of the cyclic affine plane Π and $N = n^2 - 1$. We now show that the study of cyclic affine planes is equivalent to the study of "affine difference sets" of order n. (This was done by Bose [2] under the additional hypothesis that Π was Desarguesian.) The connection between cyclic projective planes and difference sets was first pointed out by Singer [7] in a paper which essentially inaugurated the subject.

The order of the cyclic collineation τ is N. Let P be any point of Π other than X. Then each point of Π other than X can be expressed uniquely as $\tau^r P$, where r runs over all residue classes mod N. If we write r in place of $\tau^r P$, the lines of the plane may be tabulated as follows:

(2.1) *The ith line containing X ($i = 0, \ldots, n$) consists of X and all $r \equiv i \pmod{n+1}$;*

(2.2) *The ith line not containing X ($i = 0, \ldots, N-1$) consists of $d_1 + i, \ldots, d_n + i \pmod N$, where the members of the "affine difference set" $\{d_\nu\}$ are residue classes mod N such that the $n^2 - n$ differences $d_\alpha - d_\beta$ ($\alpha \neq \beta$) are precisely the $n^2 - n$ residues mod N which are not $0 \pmod{n+1}$. Further, the $\{d_\nu\}$ are in "standard form":*

$$d_\nu \not\equiv 0 \pmod{n+1}, \qquad \nu = 1, \ldots, n.$$

Received January 29, 1951. This work was done under a grant from ONR.

Proof. Let m be the smallest positive power of τ leaving PX fixed. It is clear that τ^r leaves PX fixed if and only if r is a multiple of m. In particular, $m|N$. Since PX contains $n-1$ points other than X, there are exactly $n-1$ distinct residue classes mod N congruent to 0 (mod m). Hence $m = n+1$, and PX contains X and all residues mod N congruent to 0 (mod $n+1$); $\tau^i PX$ contains X and all residues mod N congruent to i (mod $n+1$). This proves (2.1).

Let l be any line of Π parallel to PX, and let the points of l be $d_1, \ldots, d_n$. Let $d \not\equiv 0 \pmod{n+1}$. Then $\tau^d l \neq l$, nor is $\tau^d l$ parallel to l. For in either case we would have $\tau^d PX = PX$, contrary to 2.1. Hence $\tau^d l$ meets l in a single point $d_\alpha \equiv d_\beta + d \pmod{N}$; thus $d_\alpha - d_\beta \equiv d \pmod{N}$. It is also easy to see that $\tau^i l = l$ if and only if $i \equiv 0 \pmod{N}$. This proves (2.2).

Conversely, if an affine difference set is given, it can be put in standard form [2], and (2.1) and (2.2) describe an affine plane with the cyclic collineation $X \to X$, $i \to i+1 \pmod{N}$. Some trivial remarks follow at once:

(2.3) *The projective extension of* Π *admits a polarity* ρ.

Proof. Define ρ to be the following correspondence: $X \leftrightarrow$ the line at infinity, the point $i \leftrightarrow$ the $(-i)$th line of (2.2), the intersection of the line at infinity with the ith line of (2.1) $\leftrightarrow$ the $(-i)$th line of (2.1).

(2.4) *A necessary and sufficient condition that* Π *be Desarguesian is that it admit a collineation that moves* X.

Proof. The necessity is clear. For the sufficiency, it is easy to verify that if the vertices of two triangles are perspective from X, and if two of the pairs of corresponding sides are parallel, then the third pair of corresponding sides is parallel. It is then obvious that the given condition is sufficient for the validity of the affine Desargues' theorem.

(2.5) *Let* s *be a number and* σ *the mapping* $\sigma : X \to X$, $i \to si \pmod{N}$. *Then a necessary and sufficient condition that* σ *be a collineation is that there exist a number* k *such that* $sd_1, \ldots, sd_n \pmod{N}$ *is a rearrangement of* $d_1 + k, \ldots, d_n + k \pmod{N}$.

Proof. The necessity is immediate. For the sufficiency, it is clear that all we need show is that $(s, N) = 1$. But the given condition implies that the set $\{sr\} = \{s(d_\alpha - d_\beta)\}$, where r runs over all residues mod N except multiples of $n+1$, is again the set $\{r\} = \{d_\alpha - d_\beta\} \pmod{N}$. If $(s, N) = t > 1$, then $s1 \equiv s(1 + N/t) \pmod{N}$, violating the condition.

A number s with the property described in (2.5) is called a *multiplier* of the difference set (or a multiplier of the plane).

3. Multipliers. We first prove a theorem conjectured by Chowla [4] in 1945. We wish to thank Dr. Gerald Estrin for a valuable suggestion contributed to the proof.

3.1. THEOREM. *$p|n$ implies p is a multiplier.*

Proof. For convenient reference, we list several ideas:

(3.1.1) If a and b are non-negative integers and m is a positive integer, then $a \equiv b \pmod m$ if and only if $x^a \equiv x^b \pmod{x^m - 1}$.

(3.1.2) If $f(x)$ is a polynomial all of whose coefficients are non-negative, and if $g(x)$ is a polynomial of degree less than m, then $f(x) \equiv g(x) \pmod{x^m - 1}$ implies that the coefficients of $g(x)$ are non-negative.

(3.1.3) $f(x) \equiv g(x) \pmod{x^m - 1}$ implies that the sum of the coefficients of $f(x)$ equals the sum of the coefficients of $g(x)$.

(3.1.4) If $d|m$, $f(x) = 1 + x^d + \ldots + x^{(m/d-1)d}$, and $g(x)$ is any polynomial, then there is a polynomial $g_1(x)$ of degree less than d such that $f(x)\, g(x) \equiv f(x)\, g_1(x) \pmod{x^m - 1}$.

(3.1.5) In the special case of (3.1.4) in which all the non-zero terms of $g(x)$ are of the form cx^{kd}, we have $g(x)\, f(x) \equiv gf(x) \pmod{x^m - 1}$, where g is the sum of the coefficients of $g(x)$.

Now for the proof proper. We may assume that $0 < d_i < N$ (recall that $\{d_r\}$ is a standard difference set), and that p is a prime. Let $\theta(x) = x^{d_1} + \ldots x^{d_n}$. Then

$$\theta(x)\theta(x^{N-1}) \equiv n + P(x)(R(x) - 1) \qquad \bmod x^N - 1, \tag{3.1.6}$$

where $P(x) = 1 + x^{n+1} + \ldots + x^{(n-1)(n+1)}$, and

$$R(x) = 1 + x + \ldots + x^n.$$

Since p is prime to $n^2 - 1$, the numbers $pd_1, \ldots, pd_n$ form an affine difference set; hence by (3.1.1)

$$\theta(x^p)\theta(x^{(N-1)p}) \equiv n + P(x)(R(x) - 1) \qquad \bmod x^N - 1. \tag{3.1.7}$$

$p|n$ and $P(x)|x^N - 1$, so we may change the modulus of (3.1.6) to the double modulus p, $P(x)$, obtaining

$$\theta(x)\theta(x^{N-1}) \equiv 0 \qquad \text{modd } p, P(x). \tag{3.1.8}$$

Hence, $\theta(x^p)\theta(x^{N-1}) \equiv \theta(x)^p\theta(x^{N-1}) \equiv \theta(x)^{p-1}\theta(x)\theta(x^{N-1}) \equiv 0 \pmod{p, P(x)}$, which can be expressed as

$$\theta(x^p)\theta(x^{N-1}) \equiv pf(x) + P(x)g(x) \qquad \bmod x^N - 1. \tag{3.1.9}$$

By (3.1.4), we may assume $g(x) = g_0 + g_1 x + \ldots + g_n x^n$, and because of the presence of the term $pf(x)$, we may take $0 \leqslant g_i \leqslant p - 1$. Further, writing $f(x) = C_0 + C_1 x + \ldots + C_{N-1}x^{N-1}$, we have $C_i > 0$, by (3.1.2). Since $R(x)|x^{n+1} - 1$, and $P(x) \equiv n - 1 \pmod{x^{n+1} - 1}$, (3.1.9) yields

$$\theta(x^p)\theta(x^{N-1}) \equiv -g(x) \qquad \text{modd } p, R(x). \tag{3.1.10}$$

On the other hand, since $d_1, \ldots, d_n$ is a standard difference set,

$$\theta(x) \equiv R(x) - 1 \qquad \bmod x^{n+1} - 1;$$

a fortiori,

$$\theta(x) \equiv -1 \qquad \text{modd } p, R(x). \tag{3.1.11}$$

From (3.1.6), we obtain

$$\theta(x)\theta(x^{N-1}) \equiv 1 \qquad \text{modd } p, R(x),$$

which combines with (3.1.11) to give

$$\theta(x^p)\theta(x^{N-1}) \equiv (-1)^{p-1} \equiv 1 \qquad \text{modd } p, R(x). \tag{3.1.12}$$

Hence the right side of (3.1.10) is congruent to the right side of (3.1.12) (modd p, $R(x)$), so using (3.1.5) with $d = 1$, we have

$$g(x) + 1 \equiv ph(x) + kR(x) \qquad \text{mod } x^{n+1} - 1, \tag{3.1.13}$$

where k is an integer (which we may take $0 \leqslant k \leqslant p-1$) and $h(x)$ is some polynomial. Hence, $g_1 = \ldots = g_n = k \equiv g_0 + 1 \pmod p$. We cannot have $g_0 + 1 = p$, for from (3.1.9) and (3.1.3), this would imply

$$n^2 = pf + (n-1)(p-1),$$

where f is the sum of the coefficients of $f(x)$; that is $p|(n-1)(p-1)$, which is impossible. Therefore, $g_0 + 1 = k$, and

$$n^2 = pf + (n-1)(nk + k - 1);$$

that is, $p|k-1$, so $k = 1$, $f = n/p$, $g(x) = R(x) - 1$. Therefore (3.1.9) can be rewritten

$$\theta(x^p)\theta(x^{N-1}) \equiv pf(x) + P(x)(R(x) - 1) \qquad \text{mod } x^N - 1. \tag{3.1.14}$$

Replace x in (3.1.14) by x^{N-1}, and from (3.1.1) obtain

$$\theta(x)\theta(x^{(N-1)p}) = pf(x^{N-1}) + P(x)(R(x^{N-1}) - 1) \quad \text{mod } x^N - 1. \tag{3.1.15}$$

The product of the left-hand sides of (3.1.14) and (3.1.15) equals the product of the left-hand sides of (3.1.6) and (3.1.7). Hence, the respective right-hand products are congruent.

$$\begin{aligned} n^2 + 2nP(x)(R(x) - 1) + P^2(x)(R(x) - 1)^2 &\equiv p^2 f(x) f(x^{N-1}) \\ &+ pP(x)[f(x)(R(x^{N-1}) - 1) + f(x^{N-1})(R(x) - 1)] \\ &+ P^2(x)(R(x) - 1)(R(x^{N-1}) - 1) \qquad \text{mod } x^N - 1. \end{aligned} \tag{3.1.16}$$

But $P(x)R(x) \equiv P(x)R(x^{N-1}) \equiv 1 + x + \ldots + x^{N-1} \pmod{x^N - 1}$. Using this and (3.1.5), (3.1.16) becomes

$$n^2 - 2nP(x) \equiv p^2 f(x) f(x^{N-1}) - pP(x)[f(x) + f(x^{N-1})] \bmod x^N - 1. \tag{3.1.17}$$

Change the modulus to $x^{n+1} - 1$, and (3.1.17) reads

$$n^2 - 2n(n-1) \equiv p^2 \bar{f}(x)\bar{f}(x^{N-1}) - p(n-1)[\bar{f}(x) + \bar{f}(x^{N-1})] \tag{3.1.18}$$

$$\bmod x^{n+1} - 1,$$

where

$$\bar{f}(x) = \sum_{i=0}^{n} e_i x^i, \quad e_i = \sum_{j=0}^{n-2} C_{j(n+1)+i}.$$

The term on the left of (3.1.18) must be the same as the constant term on the right of (3.1.18) after reduction mod $x^{n+1} - 1$. Therefore,

$$n^2 - 2n(n-1) = p^2 \sum_{i=0}^{n} e_i^2 - 2p(n-1)e_0.$$

Add $(n-1)^2$ to both sides. Then

$$1 = p^2 \sum_{i=1}^{n} e_i^2 + [pe_0 - (n-1)]^2.$$

Hence $e_1 = \ldots = e_n = 0$. Therefore,

$$f(x) = C_0 + C_{n+1}x^{n+1} + \ldots + C_{(n-1)(n+1)}x^{(n-1)(n+1)}.$$

By (3.1.5), this implies

$$P(x)f(x) \equiv P(x)f(x^{N-1}) \equiv \frac{n}{p}P(x) \qquad \bmod x^N - 1.$$

Therefore, (3.1.17) becomes

$$n^2 \equiv p^2 f(x)f(x^{N-1}) \qquad \bmod x^N - 1,$$

and recalling that the coefficients of $f(x)$ are non-negative, this obviously implies that $f(x)$ consists of a single term, say

$$f(x) = \frac{n}{p}x^{t(n+1)}.$$

Substituting in (3.1.14),

$$\theta(x^p)\theta(x^{N-1}) \equiv nx^{t(n+1)} + P(x)(R(x) - 1) \qquad \bmod x^N - 1. \tag{3.1.19}$$

But by (3.1.1), this means that n of the differences $pd_\alpha - d_\beta$ have the same value mod N, namely, $t(n+1)$. Further, if $pd_\alpha - d_\beta \equiv pd_\mu - d_\nu \pmod N$, then $\alpha = \mu$ if and only if $\beta = \nu$. Hence the set of numbers $pd_1, \ldots, pd_n$ is a rearrangement of $d_1 + t(n+1), \ldots, d_n + t(n+1) \pmod N$. By (2.5), p is a multiplier.

3.2. THEOREM. *Let σ be the collineation of Π corresponding to the multiplier s. The fixed elements of σ form a sub-plane Π_1 if and only if $(s-1, n+1) > 3$. In this case, $(s-1, N) = ((s-1, n+1) - 1)^2 - 1$.*

Proof. Since σ leaves X fixed, the set of fixed elements forms a sub-plane Π_1, if and only if σ fixes at least three lines of (2.1), that is, if and only if $sx \equiv x \pmod{n+1}$ has at least three solutions, which is equivalent to $(s-1, n+1) > 3$. The second part of the theorem follows from a simple counting.

It is also possible to show that Π_1 is cyclic, and every multiplier of Π is also a multiplier of Π_1, but we omit the details.

3.3. THEOREM. *There is always at least one line of (2.2) left fixed by all multipliers.*

Proof. Let n be even. Then 2 is a multiplier, and the corresponding collineation fixes X, 0, the intersection of $X0$ and the line at infinity, and no other points

of the projective extension of Π. It fixes the line $X0$ and the line at infinity, so by a theorem of Baer [**1**, p. 155] exactly one other line must be left fixed. This line must be parallel to $X0$ (and hence belong to (2.2)), or another point would be fixed. By the reasoning of Hall [**6**, p. 1089], this line is fixed by all multipliers.

Let n be odd. Then S is a multiplier only if S is odd, so the $\frac{1}{2}(n+1)$th line of (2.1) is fixed by all multipliers. Therefore the line of (2.2) containing 0, parallel to this line, is fixed by all multipliers.

4. Non-existence theorems. It is known from the projective case that the preceding results imply that, for various values of n, there is no cyclic affine plane with n points on a line.

4.1. COROLLARY. *There is no cyclic affine plane with n points on a line if n is divisible by both of the primes in any one of the following pairs:*

(2,3), (2,5), (2,7), (2,11), (2,13), (2,17), (2,19), (2,23), (2,29), (2,31), (2,47), (2,61), (2,67), (2,71), (2,79), (3,5), (3,7), (3,11), (3,13), (3,17), (3,19), (3,29), (5,7), (5,11), (5,13), (5,29).

Proof as in [**6**, p. 1089].

4.2. COROLLARY. *There is no cyclic affine plane with n points on a line if there exist primes p and q such that $n \equiv 1 \pmod{p}$, $p \equiv 3 \pmod 4$, q divides the square-free part of n and $(-p|q) = 1$.*

4.3. COROLLARY. *There is no cyclic affine plane with n points on a line if n is not a square and there is an odd prime p such that* (i) $n \equiv 1 \pmod{p}$, *and* (ii) *some product of divisors of n is a primitive root of p.*

Proof. Let $\epsilon = e^{2\pi i/p}$. Substituting in (3.6), we have $\theta(\epsilon)\,\overline{\theta(\epsilon)} = \theta(\epsilon)\,\theta(\epsilon^{-1}) = n$; 4.2 then follows from the method of Chowla and Ryser [**4**, p. 95]; 4.3 follows from the method of Hall [**6**, p. 1089].

The theorems of this section, and the celebrated theorem of Bruck and Ryser [**3**], which established the non-existence of affine planes (whether cyclic or not) for various values of the number of points on a line, along with 3.2, are sufficient to decide the question of existence for all $n < 212$.

5. Remark. It is natural in the context of investigations on cyclic planes to inquire what can be said about an affine plane that admits a collineation cyclic on *all* its points. The answer is easily given: such a plane can only have two points on a line. We leave to the reader the proof that no infinite plane has this property. Here is a sketch of the proof for finite planes, with n points on a line:

Designating the points of the plane by residue classes mod n^2 in the familiar manner, it turns out, using the theorem of Baer quoted in 3.3 and the methods of §2, that the plane contains one pencil of n parallel lines such that the ith line consists of all residues congruent to $i \pmod n$. Further, if l is any other line, with points $d_0, \ldots, d_{n-1}$, then the differences $d_\alpha - d_\beta$ $(\alpha \neq \beta)$ yield all residues mod n^2 exactly once, except multiples of n. Accordingly, we choose our notation

so that $d_i \equiv i \pmod{n}$. Now precisely n of these differences will yield residues mod n^2 which are congruent to 1 (mod n), namely,

$$\begin{aligned} d_1 - d_0 &\equiv a_0 n + 1, \\ d_2 - d_1 &\equiv a_1 n + 1, \\ &\cdots \qquad\qquad \cdots \\ d_0 - d_{n-1} &\equiv a_{n-1} n + 1 \end{aligned} \qquad \pmod{n^2}. \tag{5.1}$$

The a^r form a complete system of residues mod n. Adding equations (5.1), we obtain

$$0 \equiv \tfrac{1}{2} n^2 (n-1) + n \pmod{n^2},$$

which is impossible if $n > 2$. For $n = 2$, such a collineation clearly exists.

References

1. R. Baer, *Projectivities of finite projective planes*, Amer. J. Math., vol. 69 (1947), 653-684.
2. R. C. Bose, *An affine analogue of Singer's Theorem*, J. Indian Math. Soc., vol. 6 (1942), 1-15.
3. R. H. Bruck and H. J. Ryser, *The nonexistence of certain finite projective planes*, Can. J. Math., vol. 1 (1949), 88-93.
4. S. Chowla, *On difference-sets*, J. Indian Math. Soc., vol. 9 (1945), 28-31.
5. S. Chowla and H. J. Ryser, *Combinatorial problems*, Can. J. Math., vol. 2 (1950), 93-99.
6. M. Hall, *Cyclic projective planes*, Duke Math. J., vol. 14 (1947), 1079-1090.
7. J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc., vol. 43 (1938), 377-385.

Institute for Advanced Study
Princeton, N.J.

FINITE PROJECTIVE GEOMETRIES

GERALD BERMAN

James Singer [12] has shown that there exists a collineation which is transitive on the $(t-1)$-spaces, that is, $(t-1)$-dimensional linear subspaces, of $PG(t, p^n)$. In this paper we shall generalize this result showing that there exist $t-r$ collineations which together are transitive on the s-spaces of $PG(t, p^n)$. An explicit construction will be given for such a set of collineations with the aid of primitive elements of Galois fields. This leads to a calculus for the linear subspaces of finite projective geometries.

1. The existence of a set of $t-s$ collineations transitive on the s-spaces of $PG(t, p^n)$. Let

$$(C) \qquad A_s \subset A_{s+1} \subset \ldots \subset A_{t-1} \subset PG(t, p^n)$$

be an ascending chain of linear subspaces of $PG(t, p^n)$, where A_i is an i-space $(s \leqslant i \leqslant t)$. A_i will be a finite projective geometry of i dimensions equivalent to $PG(i, p^n)$. By Singer's theorem there exists a collineation χ_i, of period $q_i = 1 + p^n + \ldots + p^{ni}$, transitive on the $(i-1)$-spaces of A_i. Let B be any s-space of $PG(t, p^n)$. Imbed B in a chain of subspaces

$$(C_0) \qquad B \equiv B_s \subset B_{s+1} \subset \ldots \subset B_{t-1} \subset PG(t, p^n).$$

By the above remarks there exists an integer ρ_t such that

$$\chi_t^{\rho_t} B_{t-1} = A_{t-1}.$$

Apply the collineation

$$\chi_t^{\rho_t}$$

to each of the spaces B_i $(i = s, s+1, \ldots, t-1)$, putting

$$\chi_t^{\rho_t} B_i = B_i^1.$$

The chain (C_0) will then be mapped on the chain

$$(C_1) \qquad B_s^1 \subset B_{s+1}^1 \subset \ldots \subset B_{t-2}^1 \subset A_{t-1} \subset PG(t, p^n).$$

Continue in this way. At the ith stage we will have the chain

$$(C_i) \qquad B_s^i \subset B_{s+1}^i \subset \ldots \subset B_{t-i-1}^i \subset A_{t-i} \subset \ldots \subset PG(t, p^n).$$

There exists an integer ρ_{t-i} such that

$$\chi_{t-i}^{\rho_{t-i}} B_{t-i-1}^i = A_{t-i-1}^i.$$

Received November 24, 1950; in revised form December 8, 1951. This paper is part of a thesis prepared under the supervision of Professor H. S. M. Coxeter and submitted for a Ph. D. degree at the University of Toronto in June, 1950.

Apply the collineation

$$\chi_{t-i}^{\rho_{t-i}}$$

to each of the spaces B_j^t $(j = s, s+1, \ldots, t-i-1)$, putting

$$\chi_{t-i}^{\rho_{t-i}} B_j^t = A_j^{t+1}.$$

The chain (C_t) will be mapped on the chain (C_{t+1}). It is clear that $(C_{t-s}) \equiv (C)$. In particular, B has been mapped by the collineation

$$\chi_{s+1}^{\rho_{s+1}} \chi_{s+2}^{\rho_{s+2}} \cdots \chi_t^{\rho_t} \text{ on } A_s.$$

The inverse collineation

$$\chi_t^{\sigma_t} \chi_{t-1}^{\sigma_{t-1}} \cdots \chi_{s+1}^{\sigma_{s+1}} \qquad (\rho_i + \sigma_i = q_i)$$

thus maps A_s on the s-space B of $PG(t, p^n)$.

Let B, B^* be any two s-spaces of $PG(t, p^n)$. We have shown that there exist collineations χ, χ^*, each products of the collineations χ_i $(i = s+1, s+2, \ldots, t)$, such that $\chi A_s = B$, $\chi^* A_s = B^*$. The collineation $\chi^* \chi^{-1}$, which is again a product of the collineations χ_i $(i = s+1, s+2, \ldots, t)$, carries B into B^*. This proves

THEOREM 1.1. *There exist $t - s$ collineations which together are transitive on the s-spaces of $PG(t, p^n)$.*

It should be noted that the collineation χ carrying A_s into B is not uniquely defined in terms of the collineations χ_i $(i = s+1, s+2, \ldots, t)$, for the chain (C_0) is arbitrary.

The purpose of the next few sections is to characterize the collineations χ_s more precisely. A method is developed for numbering the points of $PG(t, p^n)$ in such a way that the points of every linear subspace can easily be obtained. It is necessary to know only the points on one i-space $E_i(0)$ and the collineation $\chi_i(0)$ defined in terms of it for each $i = 1, 2, \ldots, t$. A construction is given for these "fundamental" s-spaces and collineations by means of primitive elements of Galois fields. The spaces $E_i(0)$ correspond to the spaces A_i above, and the collineations $\chi_i(0)$ to the collineations χ_i.

2. The representation of the points of $PG(s, p^n)$ by elements of $GF(p^{(s+1)n})$. A point of $E_s \equiv PG(s, p^n)$ may be represented analytically by an ordered sequence $P \equiv (x_0, x_1, \ldots, x_s)$ of $s+1$ elements taken from $F \equiv GF(p^n)$, the symbol $0 \equiv (0, 0, \ldots, 0)$ being excluded. If λ is any non-zero element of F, the sequence

$$\lambda P \equiv (\lambda x_0, \lambda x_1, \ldots, \lambda x_s)$$

represents the same point as P. The points

$$P_i \equiv (x_0^i, x_1^i, \ldots, x_s^i) \qquad (i = 1, 2, \ldots, n)$$

are said to be linearly dependent with respect to F if there exist r elements

λ_i $(i = 1, 2, \ldots, r)$ in F, not all zero, such that

$$\sum_{i=1}^{r} \lambda_i P_i = \left(\sum_{i=1}^{r} \lambda_i x_0^{\,i}, \sum_{i=1}^{r} \lambda_i x_1^{\,i}, \ldots, \sum_{i=1}^{r} \lambda_i x_s^{\,i} \right) = 0.$$

Otherwise the points are said to be linearly independent with respect to F. Consistent with this, an r-space $(r < s)$ is defined to be the totality of points linearly dependent upon $r + 1$ linearly independent elements of F. A point is thus a 0-space, and a line a 1-space.

Let α_s be a primitive element of $K_s \equiv GF(p^{(s+1)n})$ [3]. Every non-zero element of K_s can then be expressed uniquely in the form

$$\alpha_s^{\,i} \qquad (0 < i < p^{(s+1)n} - 2).$$

Since α_s must satisfy an irreducible F-polynomial of degree $s + 1$, $\alpha_s^{\,s+1}$ may be expressed uniquely in the form

$$\alpha_s^{\,s+1} = a_0 + a_1\alpha_s + \ldots + a_s\alpha_s^{\,s} \qquad (a_i \in F; i = 0, 1, \ldots, s).$$

With the aid of this relation, every power of α_s may be expressed uniquely in the form

$$\alpha_s^{\,i} = a_0^{(i)} + a_1^{(i)}\alpha_s + \ldots + a_s^{(i)}\alpha_s^{\,s} \equiv a^i(\alpha_s) \quad (i = 0, 1, \ldots, p^{(s+1)n} - 2)$$

where $a_j^{(i)}$ $(i = 0, 1, \ldots, p^{(s+1)n} - 2; j = 0, 1, \ldots, s)$ belong to F. This means that to every integer i $(0 < i < p^{(s+1)n} - 2)$ there corresponds uniquely an ordered sequence $(a_0^{(i)}, a_1^{(i)}, \ldots, a_s^{(i)})$ of $s + 1$ elements of F. Conversely, every ordered sequence of $s + 1$ elements of F uniquely determines one of these integers i.

We thus have four ways of denoting the elements of K_s which are uniquely defined in terms of a primitive element α_s:

(i) by the powers $\alpha_s^{\,i}$ of a primitive element;
(ii) by polynomials $a^i(\alpha_s)$ which are of degree less than $s + 1$;
(iii) by ordered sequences $(a_0^{(i)}, a_1^{(i)}, \ldots, a_s^{(i)})$ of elements of F;
(iv) by the integer i appearing in (i).

In the subsequent discussion α_s will be kept fixed, and the four notations will be used interchangeably. Since all Galois fields of the same order are isomorphic we may choose any primitive element of K_s to be α_s.

It follows from the above discussion that the points of E_s may be represented by the elements of K_s, two elements of K_s representing the same point if and only if they are linearly dependent with respect to F. An r-space of E_s $(r < s)$ will then be represented by the totality of elements of K_s linearly dependent with respect to F on $r + 1$ linearly independent elements of K_s. Corresponding to the four notations for the elements of K_s there will be four notations for the points of E_s.

The representation of the points of E_s by integers is of especial interest because of the following

THEOREM 2.1. *The integers* $0, 1, \ldots, q_s - 1$ $(q_s = 1 + p^n + \ldots + p^{sn})$ *represent different points of* E_s *and so represent all the points of* E_s.

We first prove

LEMMA 2.1. *The non-zero elements of* K_s *which correspond to the elements of* F *are the multiples of* q_s.

Let α_s^c be the element of $F \subset K_s$ having the lowest positive exponent. Then α_s^{ic} $(i = 0, 1, \ldots, g - 1;\ s^{gc} = 1)$ are elements of F. Let α_s^e be a non-zero element of F not included among these; α_s^e must occur between two successive powers of x^c, with $(k-1)c < e < kc$, so that $kc - e < c$. Then $\alpha_s^{kc-e} = \alpha_s^{kc}\,\alpha_s^{-e}$ is an element of F having lower exponent than c. The set

$$\alpha_s^{ic} \qquad (i = 0, 1, \ldots, g - 1)$$

must contain the $p^n - 1$ non-zero elements of F, so that $g = m - 1$ and

$$c = (p^{(s+1)n} - 1)/(p^n - 1) = q_s.$$

In the integer notation this means that the non-zero elements of F are the multiples of q_s.

Theorem 2.1 follows at once; for if the points $0, 1, \ldots, q_{s-1}$ are not distinct, two of them, say i and j $(i \leqslant j)$, must be linearly dependent with respect to F. By the Lemma this implies that

$$j \equiv i + kq_s \pmod{p^{(s+1)n} - 1},$$

so that $j - i$ $(0 \leqslant j - i < q_s)$ is an element of F. This can happen only if $i = j$.

Since i and j represent the same point of E_s if and only if $j \equiv i + kq_s$ for some integer k, we have

COROLLARY 2.1. *Two integers represent the same point of* E_s *if and only if they are congruent modulo* q_s.

The points of E_s may thus be represented by the residue classes of integers modulo q_s.

3. Fundamental difference sets. Let ϕ_s be the (1-1) mapping which carries any element $(a_0, a_1, \ldots, a_s)$ of K_s $(s < t)$ into the corresponding element $(a_0, a_1, \ldots, a_s, 0, \ldots, 0)$ of K_t.

$$\phi_s: \qquad (a_0, a_1, \ldots, a_s) \in K_s \rightarrow (a_0, a_1, \ldots, a_s, 0, \ldots, 0) \in K_t.$$

The inverse mapping ϕ_s^{-1} will be defined only in the image set $\phi_s K_s$, that is, for the elements $(a_0, a_1, \ldots, a_t) \in K_t$ with $a_i = 0$ $(i = s + 1, s + 2, \ldots, t)$.

If $\phi_s A_i = A_i^*$ $(i = 1, 2, \ldots, r)$, where the A_i are elements of K_s, and if $c_i \in F$, it is clear that

$$\phi_s \sum_{i=1}^{r} c_i A_i = \sum_{i=1}^{r} c_i A_i^*,$$

so that ϕ_s preserves linear independence with respect to F. Geometrically this means that ϕ_s is a collineation between E_s and a subspace of E_t.

THEOREM 3.1. *ϕ_s is a collineation between E_s and s-space of E_t.*

Since a collineation carries r-spaces into r-spaces, we have

COROLLARY 3.1. *ϕ_s carries r-spaces ($r \leqslant s \leqslant t$) of E_s into r-spaces of E_t.*

It will be convenient to order the sets of points in the subsequent discussion. The letter D will always refer to an ordered set of points, and the letter E to the same set of points considered as an unordered set.

Let D_s be the set of points E_s with the ordering $0, 1, \ldots, q_s - 1$. The collineation ϕ_s will carry D_s into an ordered subset of E_t which will be denoted by $D_s(0)$ ($D_t(0) \equiv D_t$). The elements of $D_s(0)$ will be denoted by $d_s{}^i \equiv d_s{}^i(0)$, where

$$d_s{}^i = \phi_s i \qquad (i = 0, 1, \ldots, q_s - 1; s = 1, 2, \ldots, t).$$

In particular, $d_t{}^i = i$ ($i = 0, 1, \ldots, q_t - 1$). $E_s(0)$ will of course be the unordered set of points $d_s{}^i$ ($i = 0, 1, \ldots, q_s - 1$). By Corollary 3.1 we have

THEOREM 3.2. *$E_s(0)$ is an s-space of E_t ($s = 1, 2, \ldots, t$).*

The actual numbers which represent the points of $E_s(0)$ will depend on the primitive element α_t used to define E_t, while the ordering of $D_s(0)$ will depend on the primitive elements α_s used to define E_s. The properties of the sets, however, will be the same for all choices of α_s and α_t.

The sets $D_s(0)$ ($s = 1, 2, \ldots, t$) will be called the *fundamental difference sets* of E_t. The set $E_{t-1}(0)$ is the same as the set which Singer called a difference set.

The following two theorems express useful properties of the sets defined above.

THEOREM 3.3. *$E_r(0) \subset E_s(0)$ provided $r < s$.*

If $r < s$ the set of elements $\{(a_0, a_1, \ldots, a_r, 0, \ldots, 0)\}$ is contained in the set of elements $\{(a_0, a_1, \ldots, a_s, 0, \ldots, 0)\}$ where the a_i range over all the elements of F. Geometrically this means that the set of points $E_r(0)$ is contained in the set $E_s(0)$.

THEOREM 3.4. *The s-space $E_s(0)$ contains the points $0, 1, \ldots, s$ but not the point $s + 1$, for $s = 1, 2, \ldots, t - 1$.*

The point $(\delta_0{}^i, \delta_1{}^i, \ldots, \delta_s{}^i)$ ($\delta_j{}^i = 0$ if $i \neq j$; $\delta_j{}^i = 1$ if $i = j$) is mapped by ϕ_s on the point $(\delta_0{}^i, \delta_1{}^i, \ldots, \delta_s{}^i, 0, \ldots, 0)$, so that $\phi_s\, i = i$ ($i = 0, 1, \ldots, s$). On the other hand, if some point

$$(a_0{}^{(i)}, a_1{}^{(i)}, \ldots, a_s{}^{(i)}) \qquad (i > s)$$

of E_s were mapped by ϕ_s on $(\delta_0{}^{s+1}, \delta_1{}^{s+1}, \ldots, \delta_t{}^{s+1})$ we would have, using the polynomial notation, $\alpha_t{}^{s+1} = a_0{}^{(i)} + a_1{}^{(i)}\alpha_t + \ldots + a_s{}^{(i)}\alpha_t{}^s$. If $s < t$ this means

that α_t satisfies an F-equation of degree less than $t+1$, contrary to the assumption that α_t is a primitive element of K_t.

4. Collineations. The cyclic permutation $(0, 1, \ldots, q_s - 1)$ will be denoted by χ_s.

THEOREM 4.1. *χ_s is a collineation in E_s.*

Let $\alpha_s^{e_i}$ $(i = 1, 2, \ldots, r)$ be any r collinear points of E_s. If $r > 2$ there exist r elements $\lambda_i \in F$ such that

$$\sum_{i=1}^{r} \lambda_i \alpha_s^{e_i} = 0.$$

Multiplying this equation by λ_s yields

$$\sum_{i=1}^{r} \lambda_i \alpha_s^{e_i+1} = 0.$$

In the integer notation this implies that if e_i $(i = 1, 2, \ldots, r)$ are collinear points of E_s, so also are $\chi_s e_i = e_i + 1$ $(i = 1, 2, \ldots, r)$, showing that χ_s is a collineation of E_s.

COROLLARY 4.1.1. *$\chi_s^\sigma \equiv \chi_s \chi_s \ldots \chi_s$ is a collineation of E_s of period $q_s/(q_s, \sigma)$.*

χ_s^σ, being the product of collineations, is a collineation. The period of χ_s^σ is the lowest integer r such that $(\chi_s^\sigma)^r = 1$. Thus r is the smallest positive integer such that $\sigma r = mq_s$, where m is an integer. Let

$$\sigma^* = \sigma/(q_s, \quad \sigma), q_s^* = q_s/(q_s, \sigma),$$

so that $\sigma^* r = mq_s^*$. Since σ^* and q_s^* are relatively prime, the least value for r is q_s^*.

COROLLARY 4.1.2. *If A is any r-space of E_r $(r \leqslant s)$, the sets of points $\chi_s^\sigma A$, $(\sigma = 1, 2, \ldots, q_s - 1)$ are r-spaces of E_s.*

The image $\chi_s(0) \equiv \phi_s \chi_s \phi_s^{-1}$ of χ_s under the mapping ϕ_s will be a collineation in E_t since ϕ_s and χ_s are both collineations. $\chi_s(0)$ is defined uniquely on the set $E_s(0)$ which it leaves invariant.

THEOREM 4.2. *$\chi_s(0)$ is a collineation in the space $E_s(0)$ of E_t.*

As in the previous theorem, there are two corollaries.

COROLLARY 4.2.1. *$\chi_s^\sigma(0) \equiv \chi_s(0)\, \chi_s(0) \ldots \chi_s(0) = \phi_s \chi_s^\sigma \phi_s^{-1}$ is a collineation of $E_s(0)$ of period $q_s/(q_s, \sigma)$.*

COROLLARY 4.2.2. *If $A(0)$ is any r-space of $E_s(0)$, the sets of points $\chi_s^\sigma(0) A(0)$ $(\sigma = 1, 2, \ldots, q_s - 1)$ are r-spaces of $E_s(0)$.*

It is convenient to have the collineation $\chi_s(0)$ expressed in terms of the elements of $E_s(0)$. Apply $\chi_s(0)$ to any element d_s^i of $E_s(0)$. Since

$$\chi_s(0)d_s^{\,i} = \phi_s\chi_s\phi_s^{-1}d_s^{\,i} = \phi_s\chi_s\, i = \phi_s(i+1) = d_s^{\,i+1},$$

$\chi_s(0)$ replaces any element $d_s^{\,i}$ $(i = 0, 1, \ldots, q_s - 1)$ of $E_s(0)$ by $d_s^{\,i+1}$ where $d_s^{\,q_s} \equiv d_s^{\,0}$. This proves

THEOREM 4.3.

$$\chi_s(0) = (d_s^{\,0}, d_s^{\,1}, \ldots, d_s^{\,q_s-1}).$$

More general collineations may now be defined. The product of collineations

$$\Lambda(\xi_s) \equiv \Lambda(\sigma_t, \sigma_{t-1}, \ldots, \sigma_{s+1}) \equiv \chi_t^{\,\sigma_t}\chi_{t-1}^{\,\sigma_{t-1}}(0)\cdots\chi_{s+1}^{\,\sigma_{s+1}}(0)$$

is a collineation defined in the space $E_{s+1}(0)$. The s-space $E_s(0)$ of $E_{s+1}(0)$ will be mapped by $\Lambda(\xi_s)$ into an s-space of E_t which will be denoted by $E_s(\xi_s)$, that is,

$$\Lambda(\xi_s)E_s(0) = E_s(\xi_s).$$

Note that $E_s(0, 0, \ldots, 0) = E_s(0)$. The elements of $E_s(\xi_s)$ will be denoted by $d_s^{\,i}(\xi_s)$, where

$$\Lambda(\xi_s)d_s^{\,i} = d_s^{\,i}(\xi_s) \qquad (i = 0, 1, \ldots, q_s - 1).$$

The image of the collineation $\chi_s(0)$ under the mapping $\Lambda(\xi_s)$ will be denoted by $\chi_s(\xi_s)$, so that

$$\chi_s(\xi_s) = \Lambda(\xi_s)\chi_s(0)\Lambda^{-1}(\xi_s).$$

To express $\chi_s(\xi_s)$ in terms of the elements of $E_s(\xi_s)$, apply $\chi_s(\xi_s)$ to any element $d_s^{\,i}(\xi_s)$ of $E_s(\xi_s)$:

$$\begin{aligned}\chi_s(\xi_s)d_s^{\,i}(\xi_s) &= \Lambda(\xi_s)\chi_s(0)\Lambda^{-1}(\xi_s)d_s^{\,i}(\xi_s)\\ &= \Lambda(\xi_s)\chi_s(0)d_s^{\,i} = \Lambda(\xi_s)d_s^{\,i+1}\\ &= d_s^{\,i+1}(\xi_s).\end{aligned}$$

Since

$$d_s^{\,q_s}(\xi_s) \equiv d_s^{\,0}(\xi_s)$$

we have

THEOREM 4.4.

$$\chi_s(\xi_s) \equiv (d_s^{\,0}(\xi_s), d_s^{\,1}(\xi_s), \ldots, d_s^{\,q_s-1}(\xi_s)).$$

There are relationships between the collineations defined above. For example, $\Lambda(\xi_s)$ may be expressed in terms of the collineations $\chi_i(\xi_i)$ $(i = s+1, s+2, \ldots, t)$.

THEOREM 4.5. *The collineation*

$$\chi_{s+1}^{\,\sigma_{s+1}}(\xi_{s+1})\chi_{s+2}^{\,\sigma_{s+2}}(\xi_{s+2})\cdots\chi_t^{\,\sigma_t} \equiv \Lambda^*(\xi_s)$$

is equivalent to the collineation $\Lambda(\xi_s)$.

The theorem is true for $s = t - 1$. Proceeding by induction we assume the theorem true for $s = k$ and prove it true for $s = k - 1$. That is, on the assump-

tion that $\Lambda(\xi_k) = \Lambda^*(\xi_k)$, we must prove that $\Lambda(\xi_{k-1}) = \Lambda^*(\xi_{k-1})$.

From the definitions and inductive assumption:

$$\Lambda(\xi_{k-1}) = \Lambda(\xi_k)\chi_k^{\sigma_k}(0)$$

and

$$\Lambda^*(\xi_{k-1}) = \chi_k^{\sigma_k}(\xi_k)\Lambda^*(\xi_k) = \chi_k^{\sigma_k}(\xi_k)\Lambda(\xi_k),$$

so that for any element d_k^i $(0 \leqslant i \leqslant q_k - 1)$ of $E_k(0)$ we have:

$$\Lambda(\xi_{k-1})d_k^i = \Lambda(\xi_k)\chi_k^{\sigma_k}d_k^i = \Lambda(\xi_k)d_k^{i+\sigma_k} = d_k^{i+\sigma_k}(\xi_k)$$

and

$$\Lambda^*(\xi_{k-1})d_k^i = \chi_k^{\sigma_k}(\xi_k)\Lambda(\xi_k)d_k^i = \chi_k^{\sigma_k}(\xi_k)d_k^i(\xi_k) = d_k^{i+\sigma_k}(\xi_k).$$

Thus for any linear subspace A or $E_k(0)$,

$$\Lambda(\xi_{k-1})A = \Lambda^*(\xi_{k-1})A,$$

which shows that $\Lambda^*(\xi_{k-1})$ is equivalent to $\Lambda(\xi_{k-1})$.

COROLLARY 4.5.

$$\chi_r^{\sigma_r}(\xi_r)\chi_{r+1}^{\sigma_{r+1}}(\xi_{r+1}) \cdots \chi_s^{\sigma_s}(\xi_s) = \chi_s^{\sigma_s}(\xi_s)\chi_{s-1}^{\sigma_{s-1}}(\xi_s, 0) \cdots \chi_r^{\sigma_r}(\xi_s, 0).$$

By the theorem,

$$\chi_r^{\sigma_r}(\xi_r)\chi_{r+1}^{\sigma_{r+1}}(\xi_{r+1}) \cdots \chi_s^{\sigma_s}(\xi_s)\Lambda(\xi_s) = \Lambda(\xi_s)\chi_s^{\sigma_s}(0)\chi_{s-1}^{\sigma_{s-1}}(0) \cdots \chi_r^{\sigma_r}(0),$$

so that

$$\begin{aligned}
&\chi_r^{\sigma_r}(\xi_r)\chi_{r+1}^{\sigma_{r+1}}(\xi_{r+1}) \cdots \chi_s^{\sigma_s}(\xi_s) \\
&\quad = [\Lambda(\xi_r)\chi_s^{\sigma_s}(0)\Lambda^{-1}(\xi_s)][\Lambda(\xi_s)\chi_{s-1}^{\sigma_{s-1}}(0)\Lambda^{-1}(\xi_s)] \cdots [\Lambda(\xi_s)\chi_r^{\sigma_r}(0)\Lambda^{-1}(\xi_s)] \\
&\quad = \chi_s^{\sigma_s}(\xi_s)\chi_{s-1}^{\sigma_{s-1}}(\xi_s, 0) \cdots \chi_r^{\sigma_r}(\xi_s, 0),
\end{aligned}$$

since for $k < s$,

$$\Lambda(\xi_s)\chi_k^{\sigma_k}(0)\Lambda^{-1}(\xi_s) = \Lambda(\eta_k)\chi_k^{\sigma_k}(0)\Lambda^{-1}(\eta_k) = \chi_k(\eta_k)$$

where $\eta_k = (\sigma_t, \sigma_{t-1}, \ldots, \sigma_{s+1}, 0, \ldots, 0) = (\xi_s, 0)$.

By means of Corollary 4.5, more general expressions for $\Lambda(\xi_k)$ may be obtained. Since they are not essential for the subsequent discussion, they will be omitted.

Theorems 3.3 and 3.4 may be generalized.

THEOREM 4.6. *$E_r(\xi_r) \subset E_s(\xi_s)$, provided $r < s$.*

Since $\chi_k^{\sigma_k}(\xi_k)$ leaves $E_k(\xi_k)$ invariant and

$$\Lambda(\xi_{k-1}) = \chi_k^{\sigma_k}(\xi_k)\Lambda(\xi_k)$$

it follows that

$$\Lambda(\xi_{k-1})E_k(0) = \chi_k^{\sigma_k}(\xi_k)\Lambda(\xi_k)E_k(0) = \chi_k^{\sigma_k}(\xi_k)E_k(\xi_k) = E_k(\xi_k).$$

Applying the operator $\Lambda(\xi_{k-1})$ to both sides of the inequality, $E_{k-1}(0) \subset E_k(0)$ (Theorem 3.3) yields $E_{k-1}(\xi_{k-1}) \subset E_k(\xi_k)$, so that

$$E_r(\xi_r) \subset E_{r+1}(\xi_{r+1}) \subset \ldots \subset E_s(\xi_s).$$

THEOREM 4.7. *The space $E_s(\xi_s)$ contains the points $\Lambda(\xi_s)i$ $(i = 0, 1, \ldots, s)$ but not the point $\Lambda(\xi_s)$ $(s+1)$.*

This follows at once from Theorem 3.4. As a special case we have

COROLLARY 4.7. *The space $E_s(\sigma) \equiv \chi_t^{\sigma} E_s(0)$ contains the points $\sigma, \sigma+1, \ldots, \sigma+s$, but not the point $\sigma+s+1$ $(\sigma = 0, 1, \ldots, q_s - 1)$.*

5. The linear subspaces of E_t. With the aid of the collineations just defined, all the subspaces of E_t may be obtained. We first prove

LEMMA 5.1. *The space of intersection of the $s-1$ $(s-1)$-spaces $E_{s-1}(k+i) = \chi_s^{k+i} E_{s-1}(0)$ $(i = 0, 1, \ldots, s-2)$ is a line for $k = 0, 1, \ldots, q_s - 1$.*

By Corollary 4.7, the r-space $E_r(\sigma)$ contains the points $\sigma, \sigma+1, \ldots, \sigma+r$, which, being linearly independent, span the space. $E_r(\sigma)$ and $E_r(\sigma+1)$ each contain the points $\sigma+1, \sigma+2, \ldots, \sigma+r$ and hence they each contain the space $E_{r-1}(\sigma+1)$ spanned by these points. By Corollary 4.7, $\sigma \notin E_r(\sigma+1)$ while $\sigma+r+1 \notin E_r(\sigma)$. It follows that $E_r(\sigma) \cap E_r(\sigma+1) = E_{r-1}(\sigma+1)$. Thus

$$\begin{aligned} E_{s-1}(k) \cap E_{s-1}(k+1) \cap \ldots \cap E_{s-1}(k+s-2) \\ = E_{s-2}(k+1) \cap E_{s-2}(k+2) \cap \ldots \cap E_{s-2}(k+s-2) \\ \ldots \qquad \ldots \\ = E_1(k+s-2) \end{aligned}$$

which is the line spanned by $k+s-2$ and $k+s-1$.

THEOREM 5.1. *The q_s $(s-1)$-spaces of E_s are $E_{s-1}(\sigma)$ $(\sigma = 0, 1, \ldots, q_s - 1)$.*

E_s contains exactly q_s $(s-1)$-spaces, whereas by Corollary 4.1.2, $E_{s-1}(\sigma)$ is an $(s-1)$-space for $\sigma = 0, 1, \ldots, q_s - 1$. To prove the theorem it will be sufficient to show that these q_s $(s-1)$-spaces are distinct.

Suppose the $(s-1)$ spaces $E_{s-1}(\sigma)$ $(\sigma = 0, 1, \ldots, q_s - 1)$ are not all different. Then for some $\tau_2 > \tau_1$, $E_{s-1}(\tau_1) = E_{s-1}(\tau_2)$, so that

$$\chi_s^{q_s - \tau_1} E_{s-1}(\tau_1) = \chi_s^{q_s - \tau_1} E_{s-1}(\tau_2).$$

That is $E_{s-1}(0) = E_{s-1}(\tau_2 - \tau_1)$, $0 < \tau_2 - \tau_1 < q_s$. Let $\tau < q_s$ be the least positive integer such that $E_{s-1}(\tau) = E_{s-1}(0)$. It is clear that q_s must be a multiple of τ, say $q_s = \lambda\tau$, so that the spaces $E_{s-1}(i\tau)$ $(i = 0, 1, \ldots, \lambda - 1)$ are identical. Choose $E_{s-1}(\mu)$ one of these sets such that $s - 1 < \mu < q_s - s + 1$. This can always be done. The elements of $E_{s-1}(\mu)$ are $d_{s-1}^{i} + \mu$ $(i = 0, 1, \ldots q_s - 1)$. Since, by Theorem 3.4, $E_{s-1}(0)$ contains the points $0, 1, \ldots, s-1$, there must exist s integers i_j $(j = 0, 1, \ldots, s-1)$ such that

$$d_{s-1}^{i_j} + \mu \equiv j \pmod{q_s}.$$

This means that

$$d_{s-1}^{q_i} \equiv j - \mu \qquad (j = 0, 1, \ldots, s-1)$$

are s consecutive integers lying in $E_{s-1}(0)$. These integers are different from any of $0, 1, \ldots, s-1$ by the choice of μ.

By the lemma, the intersection of the $s-1$ $(s-1)$-spaces $E_{s-1}(\sigma)$ $(\sigma = 0, 1, \ldots, s-2)$ is a line L_1, and the intersection of the $(s-1)$-spaces $E_{s-1}(\sigma)$ $(\sigma = 1, 2, \ldots, s-1)$ is a line L_2. These lines are different, for otherwise $E_{s-1}(0)$ would contain the point s. With the aid of Corollary 4.7 it is seen that L_1 and L_2 contain the points $s-1$ and $q_s - \mu + s - 1$. Since $\mu \not\equiv 0 \pmod{q_s}$ the lines L_1 and L_2 intersect in two distinct points, which is impossible. It follows that the q_s $(s-1)$-spaces $E_{s-1}(\sigma)$ $(\sigma = 0, 1, \ldots, q_s - 1)$ are different.

A more general theorem is obtained by applying the collineation $\Lambda(\xi_s)\phi_s$ to the $(s-1)$-spaces of E_s.

THEOREM 5.2. *The q_s $(s-1)$-spaces of $E_s(\xi_s)$ are $E_{s-1}(\xi_s, \sigma)$ $(\sigma = 0, 1, \ldots, q_s - 1)$.*

Here again it is sufficient to show that the q_s spaces $E_{s-1}(\xi_s, \sigma)$ are different. Suppose $E_{s-1}(\xi_s, \alpha) = E_{s-1}(\xi_s, \beta)$ $(0 \leqslant \alpha < \beta \leqslant q_s - 1)$. Apply the collineation $\phi_s^{-1}\Lambda^{-1}(\xi_s)$ to both spaces. This would mean that in the space E_s we would have $E_{s-1}(\alpha) = E_{s-1}(\beta)$ contrary to Theorem 5.1.

All the linear subspaces of $E_s(\xi_s)$ may be obtained inductively with the aid of Theorem 5.2. The $(s-1)$-spaces of $E_s(\xi_s)$ are

$$E_{s-1}(\xi_s, \sigma_s) \equiv E_{s-1}(\xi_{s-1}) \qquad (\sigma_s = 0, 1, \ldots, q_s - 1).$$

The $(s-2)$-spaces of $E_{s-1}(\xi_{s-1})$ are

$$E_{s-2}(\xi_{s-1}, \sigma_{s-1}) \equiv E_{s-2}(\xi_{s-2}) \quad (\sigma_{s-1} = 0, 1, \ldots, q_{s-1} - 1),$$

and so on. Since there is at least one descending chain of subspaces joining $E_s(\xi_s)$ with each of its r-spaces $(r = 1, 2, \ldots, s-1)$, every linear subspace may be obtained in this way.

THEOREM 5.3. *Every r-space $(1 \leqslant r < s \leqslant t)$ of $E_t(\xi_s)$ may be expressed in the form $E_r(\xi_s, \sigma_s, \sigma_{s-1}, \ldots, \sigma_{r+1})$ $(0 \leqslant \sigma_i \leqslant q_i - 1)$.*

COROLLARY 5.3.1. *Every s-space of E_t may be expressed in the form $E_s(\xi_s)$ for an appropriate choice of ξ_s.*

COROLLARY 5.3.2. *The collineation $\Lambda(\xi_s)$ maps $E_s(0)$ on any s-space of E_t for an appropriate choice of ξ_s.*

We have thus constructed a set of $t - s$ collineations $\chi_i(0)$ $(i = s+1, s+2, \ldots, t)$, the existence of which was proved in Theorem 1.1, which are transitive on the s-spaces of E_t.

DIFFERENCE SETS

$PG(2, 2)$ $D_1(0) = 0, 1, 3.$

$PG(3, 2)$ $D_1(0) = 0, 1, 4.$
$D_2(0) = 0, 1, 2, 4, 5, 10, 8.$

$PG(4, 2)$ $D_1(0) = 0, 1, 12.$
$D_2(0) = 0, 1, 2, 12, 13, 27, 24.$
$D_3(0) = 0, 1, 2, 3, 12, 13, 14, 10, 24, 25, 27, 28, 5, 18, 8.$

$PG(5, 2)$ $D_1(0) = 0, 1, 6.$
$D_2(0) = 0, 1, 2, 6, 7, 26, 12.$
$D_3(0) = 0, 1, 2, 3, 6, 7, 8, 35, 12, 13, 26, 27, 18, 48, 32.$
$D_4(0) = 0, 1, 2, 3, 4, 18, 19, 16, 32, 33, 35, 36, 6, 7, 8, 9, 56, 24, 48, 49, 38, 45, 41, 52, 12, 13, 14, 26, 27, 28, 54.$

$PG(2, 3)$ $D_1(0) = 0, 1, 9, 3.$

$PG(3, 3)$ $D_1(0) = 0, 1, 26, 32.$
$D_2(0) = 0, 1, 2, 32, 33, 12, 24, 29, 5, 26, 27, 22, 18.$

$PG(4, 3)$ $D_1(0) = 0, 1, 69, 5.$
$D_2(0) = 0, 1, 2, 5, 6, 17, 10, 101, 46, 69, 70, 88, 74.$
$D_3(0) = 0, 1, 2, 3, 22, 46, 47, 28, 36, 112, 79, 30, 138, 18, 93, 49, 15, 109, 74, 75, 39, 106, 88, 89, 10, 11, 69, 70, 71, 101, 102, 115, 5, 6, 7, 61, 77, 51, 86, 95.$

$PG(2, 4)$ $D_1(0) = 0, 1, 16, 4, 14.$

$PG(3, 4)$ $D_1(0) = 0, 1, 27, 16, 7.$
$D_2(0) = 0, 1, 2, 46, 16, 17, 51, 14, 32, 34, 4, 54, 64, 56, 7, 8, 27, 28, 23, 68, 43.$

$PG(2, 5)$ $D_1(0) = 0, 1, 10, 3, 26, 14.$

$PG(3, 5)$ $D_1(0) = 0, 1, 76, 43, 46, 18.$
$D_2(0) = 0, 1, 2, 43, 44, 122, 86, 70, 7, 64, 76, 77, 23, 119, 18, 19, 55, 61, 96, 143, 152, 92, 84, 61, 94, 108, 46, 47, 36, 89, 148.$

$PG(2, 7)$ $D_1(0) = 0, 1, 52, 3, 36, 43, 32, 13.$

$PG(2, 8)$ $D_1(0) = 0, 1, 67, 11, 38, 20, 59, 43, 71.$

$PG(2, 9)$ $D_1(0) = 0, 1, 56, 27, 49, 81, 61, 77, 3, 9.$

$PG(2, 11)$ $D_1(0) = 0, 1, 114, 100, 53, 96, 30, 131, 40, 46, 25, 122.$

$PG(2, 13)$ $D_1(0) = 0, 1, 139, 153, 119, 134, 24, 59, 128, 107, 8, 37, 41, 181.$

$PG(2, 16)$ $D_1(0) = 0, 1, 41, 147, 259, 184, 211, 70, 19, 138, 243, 80, 158, 93, 36, 267, 271.$

6. A construction for the points of the r-spaces of $E_s(\xi_s)$ $(1 \leqslant r < s \leqslant t)$ by means of difference sets. Since

$$\Lambda(\xi_r) = \chi_t^{\sigma_t}\chi_{t-1}^{\sigma_{t-1}}(0)\cdots\chi_{r+1}^{\sigma_{r+1}}(0)$$

and

$$\chi_k(0) = (d_k^0, d_k^1, \ldots, d_k^{q_k-1})$$

it is clear that all the r-spaces of $E_s(\xi_s)$ may be constructed from the sets $D_i(0)$ $(i = r, r+1, \ldots, t)$.

However, if $\xi_s \neq 0$ it is more convenient to calculate first the sets

$$D_i(\xi_s, 0) = \Lambda(\xi_s)D_i(0) \qquad (i = r, r+1, \ldots, s),$$

which by Theorem 4.4 yield the collineations $\chi_i(\xi_s, 0)$ $(i = r, r+1, \ldots, s)$. Then

$$\begin{aligned} E_r(\xi_s, \sigma_s, \sigma_{s-1}, \ldots, \sigma_{r+1}) &= \Lambda(\xi_s, \sigma_s, \sigma_{s-1}, \ldots, \sigma_{r+1})E_r(0) \\ &= \chi_{r+1}^{\sigma_{r+1}}(\xi_{r+1})\chi_{r+2}^{\sigma_{r+2}}(\xi_{r+2})\cdots\chi_s^{\sigma_s}(\xi_s)\Lambda(\xi_s)E_r(0) \\ &= \chi_s^{\sigma_s}(\xi_s)\chi_{s-1}^{\sigma_{s-1}}(\xi_s, 0)\cdots\chi_{r+1}^{\sigma_{r+1}}(\xi_s, 0)E_r(\xi_s, 0), \end{aligned}$$

by Theorem 4.5 and its Corollary.

The accompanying table of difference sets has been constructed with the aid of Galois tables [**1**; **2**] as described in §3.

References

1. W. H. Bussey, *Tables of Galois fields*, Bull. Amer. Math. Soc., vol. 12 (1905-6), 22-38.
2. ———, *Tables of Galois fields*, Bull. Amer. Math. Soc., vol. 16 (1909-10), 188-206.
3. R. D. Carmichael, *Introduction to the theory of groups of finite order* (Boston, 1937).
4. H. S. M. Coxeter, *The real projective plane* (New York, 1949).
5. ———, *Self-dual configurations and regular graphs*, Bull. Amer. Math. Soc., vol. 56 (1950), 413-456.
6. G. Fano, *Sui postulati fondamentali della geometria proiettiva in uno spazio lineare a un numero qualunque di dimensioni*, Giornale di Mathematiche, vol. 30 (1892), 106-132.
7. Marshall Hall, Jr., *Cyclic projective planes*, Duke Math. J., vol. 14 (1947), 1079.
8. W. V. D. Hodge and D. Pedoe, *Methods of algebraic geometry*, vol. 1 (Cambridge, 1947).
9. C. R. Rao, *Finite geometries and certain derived results in the theory of numbers*, Proc. Nat. Inst. Sci. India (1945), 136-149.
10. ———, *Difference sets and combinatorial arrangements derivable from finite geometries*, Proc. Nat. Inst. Sci. India (1946), 123-135.
11. G. de B. Robinson, *The foundations of geometry* (Toronto, 1940).
12. J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc., vol. 43 (1938), 377-385.
13. E. Snapper, *Periodic linear transformations of affine and projective geometries*, Can. J. Math., vol. 2 (1950), 149-151.
14. D. M. Y. Sommerville, *An introduction to the geometry of n dimensions* (London, 1929).
15. B. L. van der Waerden, *Moderne Algebra* (Berlin, 1931).
16. O. Veblen and W. H. Bussey, *Finite projective geometries*, Trans. Amer. Math. Soc., vol. 7 (1906), 244.

Illinois Institute of Technology

THE FACTORS OF GRAPHS

W. T. TUTTE

1. Introduction. A *graph* G consists of a non-null set V of objects called *vertices* together with a set E of objects called *edges*, the two sets having no common element. With each edge there are associated just two vertices, called its *ends*. Two or more edges may have the same pair of ends.

G is *finite* if both V and E are finite, and *infinite* otherwise.

The *degree* $d_G(a)$ of a vertex a of G is the number of edges of G which have a as an end. G is *locally finite* if the degree of each vertex of G is finite. Thus the locally finite graphs include the finite graphs as special cases.

A *subgraph* H of G is a graph contained in G. That is, the vertices and edges of H are vertices and edges of G, and an edge of H has the same ends in H as in G. A *restriction* of G is a subgraph of G which includes all the vertices of G.

A graph is said to be *regular of order* n if the degree of each of its vertices is n. An *n-factor* of a graph G is a restriction of G which is regular of order n.

The problem of finding conditions for the existence of an n-factor of a given graph has been studied by various authors [3; 4; 5]. It has been solved, in part, by Petersen for the case in which the given graph is regular. The author has given a necessary and sufficient condition that a given locally finite graph shall have a 1-factor [6; 7]. In this paper we establish a necessary and sufficient condition that a given locally finite graph shall have an n-factor, where n is any positive integer. Actually we obtain a more general result. We suppose given a function f which associates with each vertex a of a given locally finite graph G a positive integer $f(a)$, and obtain a necessary and sufficient condition that G shall have a restriction H such that $d_H(a) = f(a)$ for each vertex a of G. The discussion is based on the method of alternating paths introduced by Petersen [4].

We also consider the problem of associating a non-negative integer with each edge of G so that for each vertex c of G the numbers assigned to the edges having c as an end sum to $f(c)$. We obtain a necessary and sufficient condition for the solubility of this problem.

My attention has been drawn to two other papers in which similar theories of factorization have been put forward. In one of these papers, Gallai [2] gives a valuable unified theory of factors and gives some new results on the factorization of regular graphs. He also claims to have obtained a necessary and sufficient condition for the existence of a 2-factor in a general locally finite graph, but leaves the discussion of this for another occasion. In the other paper Belck [1] establishes a necessary and sufficient condition for the existence of an n-factor in a general finite graph, where n is any positive integer. Prominent

Received February 20, 1951.

in his theory is the *hyper-n-prime* graph, a generalization of the *hyperprime* graph introduced in [6].

2. **Recalcitrance.** A *path* in a graph G is a finite sequence

$$P = (a_1, A_1, a_2, A_2, \ldots, A_{r-1}, a_r) \tag{1}$$

satisfying the following conditions:

(i) The members of P are alternately vertices and edges of G, the terms $a_1, a_2, \ldots, a_r$ being vertices.

(ii) If $1 \leqslant i < r$, then a_i and a_{i+1} are the two ends of A_i.

We say that P is a path *from* a_1 *to* a_r, and that its *length* is $r - 1$. We note that the terms of P need not be all distinct. We admit the case in which P has length 0. Then P has just one term, a vertex of G.

The vertices x and y of G are *connected in* G if a path from x to y in G exists. If this is so for each pair $\{x, y\}$ of vertices of G, then G is *connected*. The relation of being connected in G is evidently an equivalence relation. It therefore partitions G into a set $\{G_\alpha\}$ of connected graphs such that each edge or vertex of G belongs to some G_α and no two of the G_α have any edge or vertex in common. We call the graphs G_α the *components* of G.

If S is any proper subset of the set of vertices of a given graph G, we denote by $G(S)$ the subgraph of G obtained by suppressing the members of S and all edges of G having one or both ends in S.

Suppose now that G is locally finite and that S is a finite set of vertices of G.

If S does not include all the vertices of G the graph $G(S)$ is defined. Then if H is any finite component of $G(S)$ we denote the number of edges which have one end in S and the other a vertex of H by $v(H)$. We have

$$v(H) + \sum_{c \in H} d_G(c) \equiv 0 \pmod 2, \tag{2}$$

for the expression on the left is equal to twice the number of edges of G having an end which is a vertex of H. (We have used the symbol $c \in H$ to denote that c is a vertex of H.)

We denote by $K(G, S)$ the set of all finite components H of $G(S)$ which satisfy

$$v(H) + \sum_{c \in H} f(c) \equiv 1 \pmod 2. \tag{3}$$

If $K(G, S)$ is finite we denote the number of its elements by $k(G, S)$. If S includes all the vertices of G we write $k(G, S) = 0$. In either case we write

$$r(G, S) = k(G, S) + \sum_{c \in S} (f(c) - d_G(c)). \tag{4}$$

We call $r(G, S)$ the *recalcitrance* of G with respect to S. If $K(G, S)$ is infinite we say that $r(G, S)$ is infinite.

THEOREM I. *If G is finite, $r(G, S)$ is even or odd according as*

$$\sum_{c \in G} f(c)$$

is even or odd.

Proof. By (2), (3), and (4),

$$r(G, S) \equiv \sum_{c \in G} d_G(c) + \sum_{c \in G} f(c) \pmod 2.$$

But the sum of the degrees of the vertices of G is even, since it is twice the number of edges of G. The theorem follows.

The locally finite graph G is *constricted* with respect to f if there exist disjoint finite sets S and T of vertices of G such that

$$\sum_{c \in T} f(c) < r(G(T), S). \tag{5}$$

As an example, G is constricted if it has a vertex a such that $d_G(a) < f(a)$. In this case (5) is satisfied if T is null and S has the single element a. Again, G is constricted if $r(G, S) > 0$ for any set S of vertices of G, for then (5) is satisfied with T null. So by Theorem I a finite graph G is constricted if the sum of the numbers $f(c)$, for all the vertices c of G, is odd. In this case (5) is satisfied if S and T are both null.

We define an *f-factor* of the given locally finite graph G as a restriction F of G such that $d_F(c) = f(c)$ for each vertex c of G. Similarly, a restriction F of a subgraph X of G is an f-factor of X if $d_F(c) = f(c)$ for each vertex c of X. A restriction F of a subgraph X of G is an *incomplete* f-factor of X if $d_F(c) \leqslant f(c)$ for each vertex c of X, and $d_F(c) = f(c)$ for all but a finite number of the vertices of X. The *deficiency* of such an incomplete f-factor is the sum

$$\sum (f(c) - d_F(c)),$$

taken over all vertices c of X for which $d_F(c) < f(c)$.

Our object in this paper is to show that G has no f-factor if and only if G is constricted with respect to f.

THEOREM II. *Let F be an incomplete f-factor of G, and let S be any finite set of vertices of G. Then the deficiency of F is not less than $r(G, S)$.*

Proof. If H is any member of $K(G, S)$, let $w(H)$ be the number of edges of F which have one end in S and the other a vertex of H. Analogously with (2) we have

$$\sum_{c \in H} d_F(c) \equiv w(H) \pmod 2. \tag{6}$$

Let P be the set of all elements H of $K(G, S)$ such that $d_F(c) = f(c)$ for each vertex c of H. Let Q be the set of all other members of $K(G, S)$. Let the numbers of members of P and Q be p and q respectively; q must be finite.

The sum of the numbers $f(c) - d_F(c)$ taken over all vertices of G not in S which satisfy $d_F(c) < f(c)$ is at least q.

If $H \in P$, then by (3) and (6), $v(H) \not\equiv w(H)$. Hence at least p of the edges of G having just one end in S are not edges of F. It follows that

$$\sum_{c \in S} d_F(c) < \sum_{c \in S} d_G(c) - p,$$

$$\sum_{c \in S} (f(c) - d_F(c)) > p + \sum_{c \in S} (f(c) - d_G(c)).$$

Hence if D is the deficiency of F we have

$$D > p + q + \sum_{c \in S} (f(c) - d_G(c)) = r(G, S).$$

THEOREM III. *If G is constricted with respect to f, it has no f-factor.*

Proof. Suppose G is constricted. Then there are disjoint finite subsets S and T of the set of vertices of G such that (5) is satisfied. Assume G has an f-factor F. Then $F(T)$ is an incomplete f-factor of $G(T)$. Its deficiency D is equal to the number n of edges of F having one end in T and the other not in T. Hence, by Theorem II,

$$\sum_{c \in T} f(c) > n = D > r(G(T), S).$$

This contradicts the definition of S and T.

3. Alternating paths. An *f-subgraph* of G is a restriction J of G having the following properties:

(i) The number of edges of J is finite.

(ii) $d_J(c) \leqslant f(c)$ for each vertex c of G.

A vertex c of G is *deficient* in J if $d_J(c) < f(c)$.

Let us suppose that we are given an f-subgraph J of G and that a is a vertex of G which is deficient in J. Following a long-established tradition we refer to an edge of G as *blue* or *red* according as it is or is not an edge of J.

An *alternating path based on a* is a path P in G which satisfies the following conditions:

(i) The first term of P is a.

(ii) No edge of G occurs twice as a term of P.

(iii) If P has more than one term the edges of G which occur in P are alternately red and blue, the first one being red.

If P includes the subsequence (c, C, d) where C is an edge of G, we say that P *passes through c and then C*, or P *passes through C and then d*.

Let $\Pi(a)$ be the set of alternating paths based on a; $\Pi(a)$ is not null since it has one member whose only term is a.

Let C be an edge of G, with ends c and d. If no member of $\Pi(a)$ has C as a term, C is *acursal*. If some member of $\Pi(a)$ passes through C and then d, C is *describable to d* or *from c*. If C is describable to d but not to c, C is *unicursal to d* or *from c*. If C is describable both to c and to d, C is *bicursal*.

A vertex of G is *accessible from a* if it is a term of some member of $\Pi(a)$.

The vertex a is *singular* if no deficient vertex of G, other than a itself, is accessible from a.

THEOREM IV. *Only a finite number of vertices of G are accessible from a.*

If b is a vertex of G accessible from a, then either $b = a$, or b is an end of a blue edge, or b is an end of an edge B whose other end is either a or an end of a blue edge. Since the number of blue edges and the degree of each vertex of G are finite, the theorem follows.

THEOREM V. *Let A and B be edges of G which are of different colours and have a common end x. Suppose A is unicursal to x. Then B is describable from x.*

There is a member P of $\Pi(a)$ which passes through A and then x. If B is not a term of P preceding A there is evidently a member of $\Pi(a)$ which agrees with P as far as A and continues $(x, B, \ldots)$. Then B is describable from x.

If B precedes A in P, either the theorem is satisfied or P passes through B and then x. In the latter case there is a member of $\Pi(a)$ which agrees with P as far as B and continues $(x, A, \ldots)$. Then A is not unicursal to x, contrary to hypothesis.

4. Bicursal components. Let us suppose that G has at least one bicursal edge.

The bicursal edges of G, with their ends, define a subgraph of G. We refer to the components of this subgraph as the *bicursal components*.

THEOREM VI. *The bicursal components are finite graphs.*

This follows from Theorem IV, since the vertices of a bicursal component are all accessible from a and G is locally finite.

Let L denote any bicursal component. An *entrant* of L is any member of $\Pi(a)$ which has a vertex of L as a term. If P is an entrant of L we denote by $e(P)$ the vertex of L which occurs first as a term of P. We then say that P *enters* L *at* $e(P)$. A vertex of L at which some entrant of L enters L is an *entrance* of L.

Let P be an entrant of L. Let A be the first edge of G in P after the first occurrence of $e(P)$ which is not in L, if such an edge exists. The *section of P by L* is defined as follows. If the edge A exists, the section is the part of P extending from the first occurrence of $e(P)$ to the term immediately preceding A. Otherwise, the section is the part of P extending from the first occurrence of $e(P)$ to the last term of P. In either case the section is an alternating path based on $e(P)$ and having only edges and vertices of L as terms (except that its first edge may be blue).

If e is any entrance of L we denote by $\Delta(e)$ the set of sections by L of those members of $\Pi(a)$ which enter L at e.

Since the edges of L are not acursal, L has at least one entrance. If a is a vertex of L then a is an entrance of L.

In the following series of theorems (VII—XI)) we suppose that some entrance e of L is specified, with the proviso that e is a if a is a vertex of L.

THEOREM VII. *There exists an edge of L which is a term of some member of $\Delta(e)$.*

Proof. Suppose first that e is a. Any red edge of L having a as an end is clearly a term of a member of $\Delta(a)$. Suppose therefore that the edges of L

having a as an end are all blue. Each of these is describable from a, and no one is the first edge of a member of $\Pi(a)$. Hence some red edge C having a as an end is describable to a. But all red edges having a as an end are describable from a. Hence C is bicursal and therefore an edge of L, contrary to supposition.

Now consider the case in which a is not a vertex of L. Let P be an entrant of L such that $e(P) = e$. Let C be the edge of G which immediately precedes the first occurrence of e in P. Then C is unicursal to e. Any edge of L having e as an end and differing in colour from C is clearly a term of a member of $\Delta(e)$. Suppose therefore that the edges of L having e as an end all have the same colour as C. Since they are all describable from e, some edge E of G differing in colour from C is describable to e. But E is describable from e, by Theorem V. Hence E is bicursal and therefore an edge of L, contrary to supposition.

THEOREM VIII. *If A is an edge of L with ends x and y, and if some member P' of $\Delta(e)$ passes through x and then A, then some other member of $\Delta(e)$ passes through y and then A.*

Proof. Since A is bicursal there exists a member Q of $\Pi(a)$ which passes through y and then A. It may happen that every term of Q which precedes A is an edge or vertex of L. Then a is a vertex of L and therefore $e = a$ by the definition of e. Hence the section of Q by L is a member of $\Delta(e)$ which passes through y and then A.

In the remaining case, let B be the last term of Q preceding A which is an edge of G but not an edge of L. Let b be the immediately succeeding term of Q. Then b is a vertex of L. Let C be the first edge of G in P' which succeeds B in Q but does not succeed A in Q. Such an edge exists since A is an edge both of P' and of Q. Let the ends of C be r and s. We may suppose that P' passes through r and then C.

Suppose Q passes through r and then C. Then there is a member of $\Delta(e)$ which agrees with P' as far as C and then continues with the terms of Q from C to A. This member of $\Delta(e)$ passes through y and then A.

Alternatively, suppose Q passes through s and then C. There is a member Q_1 of $\Pi(a)$ which enters L at e, then agrees with P' as far as C, and continues with the terms of Q in reverse order from C to b. Let D be the edge of Q_1 immediately preceding the first occurrence of e. If $B \neq D$ it follows that B is describable from b. But Q passes through B and then b. So B is bicursal and therefore an edge of L, contrary to its definition. We conclude that $B = D$ and therefore $b = e$. Hence there is a member of $\Pi(a)$ which agrees with Q_1 as far as B and agrees with Q from B to A. The section of this path by L is a member of $\Delta(e)$ which passes through y and then A.

THEOREM IX. *Let A be an edge of L which is a term of some member of $\Delta(e)$. Let x be an end of A distinct from e. Then there is an edge B of L which differs in colour from A, which has x as an end, and which is a term of some member of $\Delta(e)$.*

Proof. By Theorem VIII there is a member of $\Delta(e)$ which passes through x and then A. The last edge preceding A in this member of $\Delta(e)$ has the required properties.

THEOREM X. *If A is any edge of L and x is any end of A, then there is a member of $\Delta(e)$ which passes through x and then A.*

Proof. Let U be the set of all edges of L occurring as terms in the members of $\Delta(e)$; U is non-null, by Theorem VII. Let V be the set of all other edges of L.

Assume that V is non-null. Since L is connected there is a vertex z of L which is an end of a member B of U and a member C of V. If z is not e we may suppose that B and C differ in colour, by Theorem IX. By Theorem VIII there is a member of $\Delta(e)$ which passes through B and then z. C is not a term of this member of $\Delta(e)$. Hence there is a member of $\Delta(e)$ which agrees with this one as far as B and then continues with z and C. This contradicts the definition of C.

Suppose now that z is e. If B and C differ in colour we obtain a contradiction as before. We deduce that all the edges of L having e as an end have the same colour. If $e = a$ it follows from Theorem VII that e is an end of some red edge of L. Then C is red. Hence there is a member of $\Delta(e)$ which has C as its first edge, contrary to assumption. If e is not a it follows from Theorem VII that there is a member P of $\Pi(a)$ entering L at e in which the first occurrence of e is immediately succeeded by an edge of L. We may take this edge to be B. Since B and C have the same colour there is a member of $\Pi(a)$ which agrees with P as far as the first occurrence of e and then continues with C. Hence C is a member of U, contrary to assumption.

We conclude that V is null. The theorem now follows from Theorem VIII.

Let G_1 denote any subgraph of G. An edge A of G is said to *touch* G_1 if A is not an edge of G_1 and just one end, say x, of A is a vertex of G_1. Such an edge A is *unicursal to* or *from* G_1 if it is unicursal to or from x respectively.

THEOREM XI. *If a is a vertex of L then all edges of G which touch L are unicursal from L. If a is not a vertex of L then there exists just one edge of G which touches L and is unicursal to L, and all other edges of G which touch L are unicursal from L.*

Proof. Let A be an edge of G which touches L. Let x be the end of A which is a vertex of L. Assume that A is not unicursal from x. We recall that $a = e$ if a is a vertex of L.

If x is not e there is an edge C of L differing in colour from A and having x as an end, by Theorem IX. This is true also if $x = e = a$. For then A is blue since it is not unicursal from a and not bicursal, and Theorem VII shows that some red edge of L has a as an end. In either of these cases it follows from Theorem X that there is a member of $\Pi(a)$ which enters L at e, whose section by L passes through C and then x, and which continues from C with the terms x and A. But A is not bicursal since it is not an edge of L. Hence A is unicursal from x, contrary to assumption.

Now suppose that $x = e$ and e is not a. By Theorem VII, there is a member P of $\Pi(a)$ which enters L at e and in which the first occurrence of e is immediately succeeded by an edge C of L. Let the edge of G which immediately precedes the first occurrence of e in P be B. Clearly B touches L and is unicursal to L.

Suppose that A and B are distinct. If A differs in colour from B it is describable from $x = e$, by Theorem V. If A and B have the same colour this differs from that of C. By Theorem X there is a member Q of $\Pi(a)$ which enters L at e, and whose section by L passes through C and then e. It is clear that A and B cannot both precede C in Q. Hence there is a member Q' of $\Pi(a)$ which agrees with Q as far as C and then continues with e and one of the edges A and B. Actually, it continues with e and A since B is unicursal to e. Hence if A and B are distinct, A is unicursal from x.

This completes the proof of the theorem.

5. Bicursal units. Let T be the set of all vertices of G which are ends of bicursal edges. Let T' be the set of all edges of G having both ends in T. Then T and T' define a subgraph G' of G. We refer to the components of G' as *bicursal units*. Evidently a bicursal component having a given vertex b is a subgraph of the bicursal unit having the vertex b. By Theorem IV the bicursal units are finite graphs.

THEOREM XII. *Let M be any bicursal unit. If a is a vertex of M then all edges of G which touch M are unicursal from M. If a is not a vertex of M then there exists just one edge of G which touches M and is unicursal to M, and all other edges of G which touch M are unicursal from M.*

Proof. Since some edges of M are bicursal there exists a member P of $\Pi(a)$ having a vertex of M as a term. Let e be the first vertex of M to occur in P. If a is not a vertex of M there is an edge E of G which immediately precedes the first occurrence of e in P. Then E touches M and is unicursal to e and M. We denote the bicursal component of which e is a vertex by L. If instead a is a vertex of M we denote the bicursal component of which a is a vertex by L.

A subgraph L' of M which is a bicursal component distinct from L is *supplied from* L if there exists a sequence $(L_1, L_2, \ldots, L_t)$ of bicursal components and a sequence $(A_1, A_2, \ldots, A_{t-1})$ of edges of M such that

(i) $L_1 = L$ and $L_t = L'$,

(ii) the L_i are subgraphs of M,

(iii) for each integer i in the range $1 \leqslant i < t$, A_i is unicursal from L_i and to L_{i+1}.

We can show that any subgraph of M which is a bicursal component distinct from L is supplied from L. For suppose it is not. Then since M is connected there is an edge B of M with ends b and c belonging to bicursal components L' amd L'', where L' is L or is supplied from L, and L'' is not L and is not supplied from L. Now B is not bicursal by the definition of a bicursal component, and is not acursal, by Theorem XI. It is not unicursal to L'', since L'' is not supplied from

L. Hence B is unicursal to L'. But this is contrary to Theorem XI since L' is either L or is supplied from L.

The Theorem now follows by the application of Theorem XI to each of the bicursal components which are subgraphs of M.

If a is not a vertex of the bicursal unit M, we call the edge of G which touches M and is unicursal to M the *entrance-edge* of M. We classify such bicursal units as *red-entrant* and *blue-entrant* according as their entrance-edges are red or blue. A bicursal unit having a as a vertex is *a-entrant*.

6. Singular vertices. In this section we suppose that a is a singular vertex.

We denote the numbers of red-entrant and blue-entrant bicursal units by k_r and k_b respectively. These numbers are finite, by Theorem IV.

Let U denote the set of all vertices of G which are not vertices of G'. Thus no bicursal edge has an end in U. Let V be the set of all members of U to which some red edge is unicursal. Let W be the set of all members of U from which some red edge is unicursal or to which some blue edge is unicursal. Clearly,

$$a \notin V. \tag{9}$$

Suppose $c \in V$. Any blue edge of G having c as an end is unicursal from c, by Theorem V. Hence, by (9), no red edge of G can be unicursal from c. There are just $f(c)$ blue edges of G which have c as an end and are therefore unicursal from c since c is accessible from, but distinct from, the singular vertex a.

Now suppose $i \in W$. If some red edge is unicursal from i then either $a = i$ or there is a blue edge unicursal to i. If $a = i$ or there is a blue edge unicursal to i, then each red edge having i as an end is unicursal from i, by Theorem V and the definition of $\Pi(a)$. Hence any red edge having i as an end is unicursal from i. Consequently no blue edge of G can be unicursal from i.

It is clear from these results that V and W are disjoint sets. By Theorem IV they are finite sets.

If $i \in W$, let $y(i)$ be the number of red edges of G unicursal from i which are entrance-edges of red-entrant bicursal units. Let $z(i)$ be the number of blue edges of G which are unicursal to i from members of V.

Let H denote the graph $G(V)$. If $i \in W$, any red edge unicursal from i is unicursal to a vertex p distinct from a. For no red edge is unicursal to a. So by Theorem V, p is either a vertex of G' or a member of V. Hence in the graph H, the number of edges having i as an end is $y(i) + (d_J(i) - z(i))$. Thus we have

$$z(i) = y(i) + (d_J(i) - d_H(i)). \tag{10}$$

By the definition of a bicursal unit the entrance-edge of any bicursal unit which is not a-entrant is unicursal either from a member of V or from a member of W.

Let λ be the number of blue edges of G unicursal from a member of V to a member of W. It is equal to the total number of blue edges unicursal from members of V less the number of the entrance-edges of the blue-entrant bicursal units. The latter number is k_b, by Theorem XII. But λ is also equal to the sum

of the numbers $z(i)$ taken over all $i \in W$. The corresponding sum of the $y(i)$ is k_r, by Theorem XII. Hence we have

$$\sum_{c \in V} f(c) = k_b + k_r + \sum_{i \in W} (d_J(i) - d_H(i)). \tag{11}$$

The bicursal units, if any, are connected finite graphs. By Theorem XII, they are components of $(G(V))(W) = H(W)$.

Let M be any bicursal unit. Write $q(M) = 0$ or 1 according as M is or is not a-entrant. Let $u(M)$ be the number of blue edges of G which touch M and let $v(M)$ be the number of edges of G which touch M and have an end in W.

Using Theorem XII we readily obtain the following results: if M is blue-entrant $q(M) = 1$ and $u(M) = v(M) + 1$, if M is red-entrant $q(M) = 1$ and $u(M) = v(M) - 1$, and if M is a-entrant $q(M) = 0$ and $u(M) = v(M)$. In each case we have

$$u(M) \equiv v(M) + q(M) \pmod 2. \tag{12}$$

The sum of $u(M)$ and the degrees in J of the vertices of M is even, since it is twice the number of blue edges of G having vertices of M as ends. Moreover, if c is a vertex of M, we have $d_J(c) = f(c)$ unless $c = a$; and a is a vertex of M if and only if $q(M) = 0$. It follows from (12) that

$$v(M) + \sum_{c \in M} f(c) + (q(M) + 1)(d_J(a) - f(a)) + q(M) \equiv 0 \pmod 2. \tag{13}$$

Referring to the definitions of §2 we see that M is a member of $K(G(V), W)$ if and only if $(q(M) + 1)(d_J(a) - f(a)) + q(M) \equiv 1 \pmod 2$. Hence M is not a member of $K(G(V), W)$ if and only if M is a-entrant ($q(M) = 0$) and the deficiency $f(a) - d_J(a)$ of a in J is even.

THEOREM XIII. *If G is not constricted there exists an a-entrant bicursal unit, and the deficiency of a in J is even.*

Proof. Suppose, first, that a is a member of U but not of W. Then no red edge of G has a as an end. Hence $d_G(a) = d_J(a) < f(a)$. But then G is constricted, contrary to hypothesis, for (5) is satisfied if we take T to be null and S to have the single element a. We conclude that either $a \in W$ or there exists an a-entrant bicursal unit.

Applying formula (4) we have

$$r(G(V), W) = k(G(V), W) + \sum_{i \in W} (f(i) - d_H(i)). \tag{14}$$

If $a \in W$ then $k(G(V), W) \geq k_b + k_r$, and $f(a) > d_J(a)$. If there exists an a-entrant bicursal unit and the deficiency of a in J is odd we have

$$k(G(V), W) \geq k_b + k_r + 1.$$

Here we have used the results proved above concerning the membership of bicursal units in $K(G(V), W)$. In each of these cases it follows that the expression on the right of (11) is less than $r(G(V), W)$. Then G is constricted, contrary to hypothesis. The theorem follows.

7. Augmentation. In this section we no longer assume that the deficient vertex a is singular.

Suppose P is a member of $\Pi(a)$ which has more than one term, and whose last term is a vertex i of G deficient in J. To *transform J by P* is to replace J by a restriction K of G, defined as follows. The edges of K consist of the blue edges of G which are not terms of P, together with the red edges of G which are terms of P.

We say the f-subgraph J is *augmentable* at the deficient vertex a if there is an f-subgraph K of G satisfying the following conditions:

(i) $d_K(a) > d_J(a)$.

(ii) If $d_J(c) = f(c)$, then $d_K(c) = f(c)$.

Suppose a is not singular. Then there is a member P of $\Pi(a)$ whose last term is a deficient vertex i of G distinct from a. Let K be the restriction of G obtained by transforming J by P. By the definition of $\Pi(a)$ we have

$$d_K(a) = d_J(a) + 1, \quad d_K(i) = d_J(i) \pm 1,$$

and $d_K(c) = d_J(c)$ if c is not a or i. Hence K is an f-subgraph of G, and J is augmentable at a.

Suppose next that a is singular and that G is not constricted. The deficiency of a in J is at least 2, by Theorem XIII. Also by Theorem XIII, a is the entrance of a bicursal unit M_0. By Theorem VII there is a red edge A of M_0 having a as an end. Since A is bicursal there is a member P of $\Pi(a)$ including at least two edges, whose last term is a and whose last edge is A. Let K be the restriction of G obtained by transforming J by P. By the definition of $\Pi(a)$ we have

$$d_K(a) = d_J(a) + 2 \leqslant f(a),$$

and $d_K(c) = d_J(c)$ if c is not a. Hence K is an f-subgraph of G, and J is augmentable at a.

Thus we have the following

THEOREM XIV. *Let J be any f-subgraph of G, and let a be any vertex of G which is deficient in J. Then either G is constricted with respect to f or J is augmentable at a.*

8. Condition for an f-factor.

THEOREM XV. *G has no f-factor if and only if it is constricted with respect to f.*

Proof. Suppose first that the locally finite graph G is constricted with respect to f. Then G has no f-factor, by Theorem III.

Suppose next that G is not constricted with respect to f. Let J_0 be the restriction of G which has no edges. Then J_0 is an f-subgraph of G.

If a vertex a of G is deficient in a given f-subgraph J of G, we can, by Theorem XIV, replace J by an f-subgraph K in which the degree of a is increased and no vertex of G which is not deficient in J is deficient in K. By repeating this process sufficiently often we can obtain an f-subgraph K' of G in which a and those vertices of G not deficient in J are not deficient.

It follows that if S is any finite set of vertices of G, we can, by the above process, build from J_0 an f-subgraph J of G in which no member of S is deficient.

The theorem follows at once in the case in which G is finite. Then we can take S to be the set of all vertices of G, and the corresponding f-subgraph J must be an f-factor of G.

If G is infinite and connected we use the following non-constructive argument. (I have replaced my original proof by a shorter one for which I am indebted to the referee.)

Let x be any vertex of G. The number of paths in G whose first term is x and which have just $2n+1$ terms, where n is any given non-negative integer, is finite since G is locally finite. Hence the set of paths in G having x as first term is denumerable. Since G is connected it follows that the set of vertices of G is denumerable, say $\{a_1, a_2, \dots\}$. By the foregoing argument, to every positive integer n there is an f-subgraph J_n such that

$$d_{J_n}(a_r) = f(a_r), \qquad r \leqslant n.$$

The set of edges of G is at most denumerable, say equal to $\{A_1, A_2, \dots\}$. Put $F_n(s) = 1$ if A_s is an edge of J_n and $F_n(s) = 0$ otherwise. Then by the diagonal process, there is an increasing sequence $n_1, n_2, \dots$ such that

$$\lim_{k\to\infty} F_{n_k}(s) = F(s)$$

exists for all s. Let J be the restriction of G whose edges are those A_s for which $F(s) = 1$. Then $d_J(a_r) = f(a_r)$ for all r, and J is an f-factor of G.

Lastly, we must consider the case in which G is infinite and not connected. We can show that no component of G is constricted with respect to f. For if this is not so, there is a component G_a of G such that for some disjoint finite subsets S and T of the set of vertices of G,

$$\sum_{c\in T} f(c) < k(G_a(T), S) + \sum_{c\in S} (f(c) - d_{G_a(T)}(c)). \tag{15}$$

Clearly each component of $G_a(T)$ is a component of $G(T)$. Hence (15) holds with $G_a(T)$ replaced by $G(T)$, so that

$$\sum_{c\in T} f(c) < r(G(T), S).$$

Thus G is constricted with respect to f, contrary to hypothesis.

Since the theorem has been proved for connected graphs it follows that each component of G has an f-factor. Hence (assuming the multiplicative axiom) there is a set Z of f-factors of components of G which contains just one f-factor of each component of G. The restriction of G whose edges are the edges of the members of Z is an f-factor of G.

9. n-factors. A necessary and sufficient condition for the existence of an n-factor of G, where n is a given positive integer, can be obtained by applying Theorem XV to the special case in which the value of $f(c)$ is n for each vertex c of G.

It is convenient to denote the number of elements of a finite set U by $\mathfrak{a}(U)$. We then obtain the following

THEOREM XVI. *G has no n-factor if and only if there exist disjoint finite sets S and T of vertices of G such that*

$$n\mathfrak{a}(T) < k(G(T), S) - \sum_{c \in S} (d_{G(T)}(c) - n). \tag{16}$$

Here $k(G(T), S)$ is the number of finite components H of $(G(T))(S) = G(S \cup T)$ for which n times the number of vertices differs in parity from the number of edges of G which have one end in S and the other end a vertex of H.

A necessary and sufficient condition for the existence of a 1-factor of a given locally finite graph G has been given in previous papers [6; 7]. It is simpler in form than the expression obtained by writing $n = 1$ in (16). In the next section, this simpler formula is deduced from Theorem XV. The argument suggests no analogous simplification in the case $n > 1$.

10. An allied problem. Suppose that we are given a locally finite graph G, and a function f which associates with each vertex c of G a positive integer $f(c)$. We consider the problem of associating with each edge A of G a non-negative integer $h(A)$ so that for each vertex c of G the sum of the numbers $h(A)$, taken over all edges A of G having c as an end, is $f(c)$. If such a set of non-negative integers $h(A)$ exists we say that G is *f-soluble*.

We note that if $f(c) = 1$ for each vertex of G, then G is f-soluble if and only if it has a 1-factor.

Let T be any finite set of vertices of G. We denote by $S(T)$ the set of all vertices c of G having the following properties:

(i) c is not an element of T.

(ii) Each edge of G having c as an end has its other end in T.

If T does not include every vertex of G we denote by $k(T)$ the number of finite components H of $G(T)$ having the following properties:

(i) H has more than one vertex.

(ii) The sum of the numbers $f(a)$, taken over all vertices of H, is odd.

If T is the set of all vertices of G we write $k(T) = 0$.

THEOREM XVII. *G is not f-soluble if and only if there exists a finite set T of vertices of G such that*

$$\sum_{c \in T} f(c) < k(T) + \sum_{c \in S(T)} f(c). \tag{17}$$

Proof. By adjoining new edges to G we can obtain a graph G' having the following properties:

(i) The vertices of G' are the vertices of G.

(ii) Two vertices are joined by an edge in G' if and only if they are joined by an edge in G.

(iii) If two vertices a and b are joined by an edge in G', the number of distinct edges of G' which join them is finite and not less than $d_G(a) + f(a)$.

Clearly G' is locally finite.

If S and T are disjoint finite sets of vertices of G such that S is contained in $S(T)$ it follows from the definition of G' that

$$k(G'(T), S) = k(G(T), S). \tag{18}$$

It is clear that G is f-soluble if and only if G' has an f-factor. Hence, by Theorem XV, G is not f-soluble if and only if there exist disjoint finite sets S and T of vertices of G such that

$$\sum_{c \in T} f(c) < k(G'(T), S) - \sum_{c \in S} (d_{G'(T)}(c) - f(c)). \tag{19}$$

Suppose first that (17) is satisfied for some finite T. If $S(T)$ is not finite then all but a finite number of its elements have degree 0 in G, since G is locally finite. Hence G is not f-soluble since it has a vertex of degree 0. If $S(T)$ is finite it follows from (17) and (18) that (19) will be satisfied if we put $S = S(T)$. Hence G is not f-soluble.

Conversely, suppose that G is not f-soluble. Then (19) is satisfied for some disjoint finite sets S and T. If possible let a be any member of S not in $S(T)$. Consider the effect of replacing S by $S' = S - \{a\}$. Clearly the replacement diminishes

$$\sum_{c \in S} (d_{G'(T)}(c) - f(c))$$

by $d_{G'(T)}(a) - f(a)$, that is, by at least $d_G(a)$, from (iii).

The replacement diminishes $k(G'(T), S)$ by not more than $d_{G(T)}(a)$, the maximum number of finite components of $G'(S \cup T)$ joined to a by an edge of G'. But $d_{G(T)}(a) \leqslant d_G(a)$. Hence, if a is not an element of $S(T)$, formula (19) remains valid when S is replaced by S'.

If S' has an element not in $S(T)$ we repeat the argument with S' replacing S, and so on. Since S is finite we find, eventually,

$$\sum_{c \in T} f(c) < k(G'(T), U) + \sum_{c \in U} f(c), \tag{20}$$

where U is the intersection of S and $S(T)$. But, by (18), $k(G'(T), U)$ is equal to $k(T)$ plus the number of components of $G(T \cup U)$ which consist of a single vertex, the value of f for this vertex being odd. Hence

$$k(G'(T), U) \leqslant k(T) + \sum_{c \in S(T) - U} f(c). \tag{21}$$

Now (20) and (21) imply (17). This completes the proof of the theorem.

If $f(c) = 1$ for each vertex c of G it is clear that G is f-soluble if and only if it has a 1-factor. Applying Theorem XVII to this case we find that G has no 1-factor if and only if there exists a finite set T of vertices of G such that

$$a(T) < h_a(T),$$

where $h_a(T)$ is the number of finite components of $G(T)$ having an odd number of vertices. This is the simple criterion for the existence of a 1-factor mentioned in §9.

References

1. H. B. Belck, *Reguläre Faktoren von Graphen*, J. Reine Angew. Math., vol. 188 (1950), 228-252.
2. T. Gallai, *On factorization of graphs*, Acta Mathematica Academiae Scientarum Hungaricae, vol. 1 (1950), 133-153.
3. P. Hall, *On representation of subsets*, J. London Math. Soc., vol. 10 (1934), 26-30.
4. J. Petersen, *Die Theorie der regulären Graphs*, Acta Math., vol. 15 (1891), 193-220.
5. R. Rado, *Factorization of even graphs*, Quarterly J. Math., vol. 20 (1949), 95-104.
6. W. T. Tutte, *The factorization of linear graphs*, J. London Math. Soc., vol. 22 (1947), 107-111.
7. ———, *The factorization of locally finite graphs*, Can. J. Math., vol. 1 (1950), 44-49.

The University of Toronto

SOME CHARACTERIZATIONS OF GENERALIZED MANIFOLDS WITH BOUNDARIES

PAUL A. WHITE

In R. L. Wilder's book [2] the open and closed generalized manifolds are extensively studied. However, no study is made of the generalized manifold with boundary nor is a definition of such a space given except in the case of the generalized closed n-cell. A definition of a generalized manifold with boundary was given by the author in his paper [1]. Before undertaking the study of further properties of these manifolds it seems appropriate to characterize the manifolds with boundary in terms of the open and closed manifolds of Wilder. It is to that purpose that this paper is directed and in particular the generalized closed n-cell of Wilder is characterized as a special manifold with boundary.

The space M that we shall deal with will be a compact Hausdorff space and the homology theory used will be that of Čech in which the coefficient group for the chains will be an arbitrary field which we shall omit from the notation for a chain. We shall use small Roman letters for points and large Roman letters for sets of points. We shall use "$\cup$" for point set union or sum, "$\cap$" for intersection, reserving $+$ and $-$ for the group operations.

1. The generalized manifold with boundary; condition D.

Definition 1. If K is a closed subset of M, then we will say that *the local r-dimensional Betti number of M at x* mod K, denoted by $p_r(M \bmod K; x)$, *is the finite integer k* if k is the smallest positive integer with the property that corresponding to any open set P such that $x \in P$ there exists an open set Q such that $x \in Q$, $\bar{Q} \subset P$, and such that any $k+1$ Čech cycles of M mod

$$(M - (P - K)) = (M - P) \cup K$$

are linearly dependent with respect to homologies on M mod

$$M - (Q - K) = (M - Q) \cup K.$$

(Note that if $K = 0$ then this definition is equivalent to the definition of $p_r(M, x)$, the local Betti number of M at x. Also this is equivalent to Wilder's definition [2, p. 291] of the Betti number around a point.)

Definition 1.2. The compact space M will be called an *n-dimensional generalized manifold* (n-gm) *with boundary* if there exists a closed subset K of M such that:

(1) $M = K \cup A$ where A is open, $K = \bar{A} - A$, and dim $K < n$, and dim $M = n$ (in the sense of Lebesque [2, p. 195],

Received October 31, 1950.

(2) $p_r(M \bmod K; x) = 0$ for all $x \in M$, $r \leqslant n-1$,
(3) $p_n(M \bmod K; x) = 1$ for all $x \in M$,
(4) $p_r(M, x) = 0$ for all $x \in K$, $r \leqslant n$.
(Note that this definition reduces to Wilder's definition of an n-dimensional generalized closed manifold (n-gcm) when $K = 0$ [2, p. 244] for (2) becomes $p_r(M, x) = 0$, $r < n$, which is equivalent to r-co-local connectedness $r < n$, and (4) no longer applies.)

THEOREM 1.1. *The boundary set K in Definition 1.2 is unique.*

Proof. Let K_1 and K_2 be two closed subsets of M satisfying the conditions of Definition 1.2. Suppose there is a point $x \in K_1$ but not $\in K_2$. By (3), $p_n(M \bmod K_2; x) = 1$, but since $x \notin K_2$, $p_n(M \bmod K_2; x) = p_n(M, x)$, hence $p_n(M, x) = 1$ which is a contradiction to $p_n(M, x) = 0$ by (4) since $x \in K_1$. Thus $K_1 = K_2$.

THEOREM 1.2. *A necessary and sufficient condition that M be a manifold with boundary is that there exist a closed subset K of M such that:*

(1) $M = K \cup A$, $K \cap A = 0$, $\dim M = n$,
(2) K is an $(n-1)$-gcm (see note after Definition 1.2),
(3) A is a non-compact n-gm (i.e., Definition 1.2 with $K = 0$ and M locally compact, but not compact),
(4) $p_r(M, x) = 0$, $r \leqslant n$ for all $x \in K$.

Proof of necessity. (1) This clearly follows from Definition 1.2 (1). (2) We first note that K is compact since $K = \bar{A} - A$ is a closed subset of the compact set M. We next show that $p_{n-1}(K, x) = 1$ for all $x \in K$ and that K is $\operatorname{colc}^{n-2}$ (that is, r-co-locally connected $r \leqslant n-2$, which is equivalent to $p_r(K, x) = 0$, $r \leqslant n-2$ for all $x \in K$). Since by Definition 1.2 (4) $p_{r-1}(M, x) = p_r(M, x) = 0$ for $r \leqslant n$ and all $x \in K$, it follows that $p_{r-1}(K, x) = p_r(M \bmod K; x)$ which [2, p. 291, Theorem 1.4] gives us the result by referring to (2) and (3) of the definition. Finally, $\dim K = n-1$, for $\dim K < n$, but if $\dim K \leqslant n-2$, then [2, p. 196, Theorem 7.7] we conclude that $p_{n-1}(K, x) = 0$ contrary to what we have just proved above.

(3) We first observe that $K \neq 0$ since $\dim K = n-1$ and, therefore, A is locally compact but not compact, since it is an open subset of a compact space M and has a non-vacuous boundary K. Also $\dim A = n$ by Definition 1.2 (3). A is clearly $\operatorname{colc}^{n-1}$ and $p_n(A, x) = 1$ for $x \in A$ by (2) and (3) since $p_r(M \bmod K; x) = p_r(M, x) = p_r(A, x)$ for $x \in A$.

(4) This is the same as Definition 1.2 (4).

Proof of sufficiency. By (1) $\bar{A} - A \subset K$ and if $x \in K$, but $x \notin \bar{A} - A$ then

$$p_{n-1}(M, x) = p_{n-1}(K, x),$$

but $p_{n-1}(M, x) = 0$ by (4) which contradicts $p_{n-1}(K, x) = 1$ by part of (2); therefore $\bar{A} - A = K$. Also $\dim K = M - 1 < M$ by (2).

By [2, p. 292, Theorem 1.4] again together with $p_{r-1}(M, x) = p_r(M, x) = 0$ for $x \in K$, $r \leqslant n$, we conclude that $p_{r-1}(K, x) = p_r(M \bmod K; x)$ for all $x \in K$.

By (2) and the above equality, we have $p_r(M \bmod K; x) = p_{r-1}(K, x) = 0$ for all $x \in K$, $r \leqslant n-1$, and for $x \in A$ this follows from (3).

By (2) and the above equality we have $p_n(M \bmod K; x) = p_{n-1}(K, x) = 1$ for all $x \in K$, which follows from (3) for $x \in A$.

This is the same as (4).

Definition 1.3. The n-gm M with boundary will be said to satisfy condition D if $p^n(M_1, K) = 0$ ($p^n(M_1, K)$ denotes the number of n-cycles on M_1 mod K linearly independent with respect to homologies on M_1 mod K), where M_1 is a proper closed subset of M. We will denote this by saying that M is an n-D-gm with boundary. (This corresponds to condition D [2, p. 250].)

THEOREM 1.3. *A necessary and sufficient condition that M be an n-D-gm with boundary is that there exists a closed subset K of M such that*:

(1) $M = K \cup A$, $K \cap A = 0$, dim $M = n$.

(2) *K is an $(n-1)$-gcm.*

(3) *A is a non-compact n-gm satisfying* D′ (i.e., if z^n is an infinite cycle of A on a subset A_1 of A closed relative to A such that the closure of $A - A_1$ relative to A is compact, then $z^n \backsim 0$ on A. See [2, p. 254]).

(4) *$p_r(M, x) = 0$, $r \leqslant n$, for all $x \in K$.*

Before proving this theorem we remark that in the case of a closed subset K of a compact space M, such as we have here, the cycles M mod K and the infinite cycles on $A = M - K$ are related in a one to one fashion so that if z^n is a cycle on M mod K and $\mathfrak{z}^n$ is the related infinite cycle on A, then $z^n \backsim 0$ on M mod K if and only if $\mathfrak{z}^n \backsim 0$ on A. This result has been verified by Wilder in connection with some of his work that is not yet published. We now proceed to the proof.

Proof of necessity. All the conditions (1), (2), (3), and (4) follow from Theorem 1.2, except that A satisfies D′. To verify this let $A_1 \subset A$ be closed relative to A, such that $\overline{A - A_1}$ relative to A is compact. Let $\mathfrak{z}^n$ be an infinite cycle on A_1, then by the above remark there is a corresponding cycle z^n on M mod K and z^n will be on $M_1 = A_1 \cup K_1$ which is a proper closed subset of M. By hypothesis $p^n(M_1, K) = 0$ implies that $z^n \backsim 0$ on M_1, hence on M_1 mod K, and by the remark $\mathfrak{z}^n \backsim 0$ on A.

Proof of sufficiency. That M is an n-gm with boundary follows from Theorem 1.2. To show that M satisfies D, let M_1 be a proper closed subset of M. Now $A \cap (M - M_1) \neq 0$, for otherwise $A \subset M_1$ and $\bar{A} = M \subset M$; also $A \cap (M - M_1)$ is open and therefore contains an open set U such that $\bar{U} \subset A \cap (M - M_1)$. If z^n is a cycle on M_1 mod K_1 then the corresponding infinite cycle $\mathfrak{z}^n$ of A is on $A - U$, which is proper closed relative to A, and

$$\overline{A - (A - U)} = \bar{U} \subset A$$

is compact. Thus $i^n \backsim 0$ on A and by the remark $z^n \backsim 0$ on M mod K, but this implies that $z^n = 0$ mod K (with respect to the n-dimensional coverings of M); hence $z^n \backsim 0$ on M_1 mod K (with respect to all coverings).

THEOREM 1.4. *If M is an n-D-gm with boundary K, then $p^n(M_1, K_1) = 0$, where M_1 and K_1 are closed subsets of M and K, respectively, and at least one subset is proper.*

Proof. It is sufficient to prove the theorem for cycles whose coordinates are restricted to a complete family of coverings of M, [**2**, p. 130], and since M is n-dimensional we can suppose this to be the family of n-dimensional coverings of M [**2**, p. 195]. First consider the case where K_1 is a proper closed subset of K. Let $p \in K - K_1$, then $p_n(M, x) = 0$ and we can choose open sets U, V such that $x \in V$, $\bar{V} \subset U$, $U \cap K_1 = 0$, and such that any n-cycle on M mod $(M - U)$ is $\backsim 0$ on M mod $(M - V)$. In particular if z^n is a cycle on M_1 mod K_1, then it is a cycle mod $(M - U)$; hence $\backsim 0$ on M mod $(M - V)$. Since only n-dimensional coverings are being used, this means that

$$z^n = 0 \mod (M - V),$$

that is, z^n is on $M - V$. Now $M - V$ is a proper closed subset of M; therefore $p^n(M - V, K) = 0$, and $z^n \backsim 0$ on $M - V$ mod K, but as before this implies that z^n is on K; hence $\backsim 0$ on M_1 mod K, that is, $p^n(M_1, K_1) = 0$. The only remaining case would be where M_1 is a proper subset of M and $K_1 = K$, then $p^n(M_1, K_1) = 0$ by hypothesis.

Remark. The condition D is actually stronger than the similar condition $p^n(M, K_1) = 0$, for proper closed subsets K_1 of K, which it implies, as is shown by letting M consist of the union of a bounded 2-cell and a disjoint projective plane.

THEOREM 1.5. *If M is an n-D-gm with boundary K, then $p^n(M, K) \leqslant 1$.*

Proof. Suppose C^n_1 and C^n_2 are cycles on M mod K linearly independent with respect to homologies on M mod K. Let $x \in M - K$, then $p_n(M, x) = p_n(M \text{ mod } K; x) = 1$ (by Definition 1.2 (3)); therefore we can find open sets V, U such that $x \in V$, $\bar{V} \subset U$, $U \cap K = 0$ and such that any two cycles mod $(M - U)$ are linearly dependent with respect to homologies mod $(M - V)$. In particular C^n_1 and C^n_2 are cycles mod $(M - U)$; hence there exist elements a_1, a_2 of the coefficient field, not both zero, such that

$$a_1 C^n_1 + a_2 C^n_2 \sim 0 \mod (M - V).$$

Again we can restrict our cycles to n-dimensional coverings of M, which implies that

$$z^n = a_1 C^n_1 + a_2 C^n_2$$

is on $M - V$. Since $M - V$ is a proper closed subset of M, and M satisfies D, we have $z^n \backsim 0$ on $M - V$ mod K contrary to the assumption that C^n_1 and C^n_2 were linearly independent mod K; thus $p^n(M, K) \leqslant 1$.

2. Orientability.

Definition 2.1. An n-gm M with boundary K is called *orientable* if M is the carrier of a cycle z^n mod K such that $z^n \sim \Gamma^n$ mod K on M where Γ^n is a cycle mod K on a proper closed subset of M. (If $K = 0$, this becomes the definition of an orientable n-gcm.)

THEOREM 2.1. *A necessary and sufficient condition that M be an orientable n-gm with boundary is that there exist a closed subset K of M such that:*

(1) $M = K \cup A$, $K \cap A = 0$, $\dim M = n$.

(2) *K is an* $(n-1)$-gcm.

(3) *A is a non-compact n-gm orientable in the sense that there is an infinite cycle on A not homologous on A to any infinite cycle on a proper closed subset of A.*

(4) $p_r(M, x) = 0$, $r \leqslant n$, *for all* $x \in K$.

(See [2, p. 254] for definition of infinite cycle on a proper closed subset.)

From Theorem 1.2 it follows that we need only show that the orientability of A is a necessary and sufficient condition for the orientability of M.

Proof of necessity. Let z^n be the cycle on M mod K given in the definition of orientability and let ζ^n be the infinite cycle on A corresponding to z^n according to the remark after the statement of Theorem 1.3. If $z^n \backsim \zeta^n{}_1$ on A where $\zeta^n{}_1$ is an infinite cycle on a proper closed subset A_1 of A, then $\zeta^n{}_1$ determines a cycle $z^n{}_1$ on $A_1 \cup K = M_1$ which is a proper closed subset of M such that $z^n \backsim z^n{}_1$ mod K on M, contrary to the hypotheses on z^n. Thus ζ^n is the required infinite cycle on A.

Proof of sufficiency. Let ζ^n be the infinite cycle on A in the definition of the orientability of A and let z^n be the cycle on M mod K corresponding to it. Suppose $z^n \backsim z^n{}_1$ on M mod K, where $z^n{}_1$ is a cycle on M_1 mod K, and M_1 is a proper closed subset of M. Then $z^n{}_1$ would correspond to an infinite cycle $\zeta^n{}_1$ on a proper closed subset A_1 of A as in the proof of Theorem 1.3, and z^n would be $\backsim \zeta^n{}_1$ on A, contrary to the hypotheses on ζ^n. Thus z^n is the required cycle on M mod K in the definition of orientability.

THEOREM 2.2. *If M is an orientable n-gm with boundary K, then K is an orientable* $(n-1)$-gcm.

Proof. K is an $(n-1)$-gcm by Theorem 1.2. To show that K is orientable, let z^n be the cycle on M mod K according to the definition of orientability; then $\partial z^n = z^{n-1}$ is a cycle on K. Suppose $z^{n-1} \backsim z^{n-1}{}_1$ on K where $z^{n-1}{}_1$ is a cycle on a proper closed subset K_1 of K. Thus $z^{n-1}{}_1 \backsim 0$ on M and by [2, p. 201, Lemma 1.4] there exists a cycle C^n mod K_1 on M such that $\partial C^n \backsim z^{n-1}{}_1$ on K_1. Choose $x \in K - K_1$, and since $p_n(M, x) = 0$, there exist open sets U, V, such that $x \in V$, $\bar{V} \subset U$, $U \cap K_1 = 0$, and such that any n-cycle mod $(M - U)$ is $\backsim 0$ mod $(M - V)$. In particular C^n is a cycle mod $(M - U)$; therefore $C^n = 0$ on V (when restricted to the complete family of n-dimensional coverings). Thus C^n

is on a proper closed subset $M_1 = M - V$ of M. Now

$$\partial C^n - \partial z^n \sim z^{n-1}{}_1 - z^{n-1} \sim 0 \text{ on } K;$$

therefore, there exists by [**2**, p. 201, Lemma 1.6] a cycle Γ^n on M such that $(C^n - z^n) \backsim \Gamma^n \bmod K$ on M. Again Γ^n is a cycle on $M \pmod{K_1}$; therefore Γ^n (when restricted to n-dimensional coverings) is on M_1 as before. Now $z^n \backsim C^n - \Gamma^n \bmod K$ on M, where $C^n - \Gamma^n$ is on M_1. It follows that z^n is $\backsim \bmod K$ to a cycle on a proper closed subset of M. This contradicts the orientability assumption; hence z^{n-1} is not homologous to a cycle on a proper closed subset of K, which is the orientability condition for K.

The orientability condition for the n-D-gm can be more simply stated as is indicated in the following theorem.

THEOREM 2.3. *A necessary and sufficient condition that an n-D-gm M with boundary K be orientable is that $p^n(M, K) = 1$.*

Proof. By Theorem 1.5, $p^n(M, K) \leqslant 1$; thus the orientability assumption, which implies $p^n(M, K) \geqslant 1$, implies $p^n(M, K) = 1$. Conversely, $p^n(M, K) = 1$ implies the existence of a cycle z^n on $M \bmod K$ which is not $\backsim 0 \bmod K$ and, therefore, is not homologous to a cycle $z^n{}_1$ on a proper closed subset M_1 of M, for any such cycle z_1 is $\backsim 0$ by property D.

In connection with the orientable n-D-gm it turns out that if condition D had been stated, "$p^n(M, K_1) = 0$, where M_1, K_1 are closed subsets of M and K, respectively, such that one but not both inclusions are proper," then the n-dimensional part of Definition 1.2 (4) follows from the other hypotheses. This is embodied in the following theorem and corollary.

THEOREM 2.4. *For an orientable n-gm M with boundary K satisfying the condition $p^n(M, K_1) = 0$ where K_1 is a proper closed subset of K, the condition $p_n(M, x_1) = 0$ for $x \in K$ in the definition of a manifold follows from the other conditions in the definition.*

Proof. It will be sufficient to prove the proposition for the complete family of n-dimensional coverings of M. Let x be any point of K and U any open set, $x \in U$, and let γ^n be an arbitrary n-cycle mod $(M - U)$, hence mod $[(M - U) \cup K]$. Since $p_n(M \bmod K, x) = 1$, there is an open set V, $\bar{V} \subset U$, $x \in V$, such that there is only one cycle mod $[(M - U) \cup K]$ linearly independent with respect to homologies on M mod $[(M - V) \cup K]$. Let z^n be the cycle on M mod K from the definition of orientability, then z^n is a cycle mod $[(M - U) \cup K]$. Also

$$z^n \nsim 0 \mod [(M - V) \cup K],$$

for otherwise it would be on $(M - V) \cup K$ (since only n-dimensional coverings are being used), contrary to the orientability assumption which says that z^n is not $\backsim$ to a cycle mod K on a proper closed subset of M. Now suppose $\gamma^n \nsim 0$ mod $[(M - V) \cup K]$ on M, then there exist elements $a_1 \neq 0$ and $a_2 \neq 0$ of the coefficient field such that $a_1\gamma^n + a_2z^n \backsim 0 \bmod [(M - V) \cup K]$ on M, but

this means that $a_1\gamma^n + a_2 z^n = 0$ on $V - K$, hence $= 0$ on

$$\overline{V - K} = \bar{V}.$$

Then $a_1\partial\gamma^n + a_2\partial z^n = 0$ on $\bar{V}$, but $\partial\gamma^n$ is on $M - U$, hence $= 0$ on $\bar{V} \subset U$; thus $\partial z^n = 0$ on $\bar{V}$. Now $K_1 = K - V$ is a proper closed subset of K and by the above z^n is a cycle mod K_1; therefore by the hypothesis $p^n(M, K_1) = 0$, we have $z^n \backsim 0$ on M mod K_1, contrary to the orientability assumption. Thus we conclude that

$$\gamma^n \sim 0 \mod [(M - V) \cup K] \text{ on } M;$$

hence $\gamma^n = 0$ on $V - K$ (since only n-dimensional coverings are considered). This, however, implies $\gamma^n = 0$ on

$$\overline{V - K} = \bar{V};$$

therefore $\gamma^n \backsim 0 \mod (M - V)$, and $p_n(M, x) = 0$ for all $x \in K$.

COROLLARY 2.4.1. *For an orientable* n-D-gm M *with boundary* K *the condition* $p^n(M, K_1) = 0$, *where* K_1 *is a proper closed subset of* K, *is equivalent to the condition* $p_n(M, x) = 0$ *for all* $x \in K$.

Proof. The proof follows by combining Theorems 1.4 and 2.4

The following example shows that condition (4) of Definition 1.2 is necessary for $r < n$ even in the case of an orientable n-D-gm.

Example. Let M be a solid pinched sphere, i.e., a 2-sphere plus its interior in which all points on some fixed diameter are identified. Let K equal the boundary 2-sphere with the pinched points, then M satisfies conditions D and (1), (2), (3), and (4) (for $r = n = 3$) of Definition 1.2, but $p_2(M, x) = 1$ where x is the pinched point.

The next theorem and its corollaries clarify the role of the n-D-gm in connection with the orientable n-gm.

3. The orientable manifold satisfying condition D.

THEOREM 3.1. *If* M *is an* n-gm *with boundary* K, *then* M *has only a finite number of components* $M_1 \cup M_2 \cup \ldots \cup M_k$, *and each component* M_i *is an* n-gm *with boundary* $K_i = K \cap M_i$; *and if* M *is orientable, then each* M_i *is an orientable* n-D-gm *with boundary* K_i.

Proof. M has only a finite number of components since it is compact and locally-0-connected. Let $A_i = M_i - K_i$, then clearly (1) $\bar{A}_i - A_i = K_i$. Conditions (2), $p_r(M_i \bmod K_i, x) = 0$ for all $x \in M_i$, $r \leqslant n - 1$; (3) $p_n(M_i \bmod K_i, x) = 1$ for all $x \in K_i$; and (4), $p_r(M_i, x) = 0$ for all $x \in K_i$, $r \leqslant n$ follow immediately from the corresponding conditions on M and K since $K_i \subset K$ and the M_i are separated. The condition dim $M_i = n$ follows since $M_i \subset M$ and dim $M = n$ implies that dim $M_i \leqslant n$, and condition (3) for M_i requires that dim $M_i \geqslant n$. Also if M is orientable, then each M_i is orientable, for the cycle

z^n in the definition of orientability of M can be written in the form

$$z^n = z^n{}_1 + \ldots + z^n{}_k,$$

where each z_i is the part of z^n on M_i and is clearly a cycle mod K_i with the properties required for the orientability of M_i.

Finally we will show that M_i satisfies condition D. To this end consider M'_i a proper closed subset of M_i. We must show $p^n(M'_i, K_i) = 0$, and it will be sufficient to consider only the complete family of n-dimensional coverings of M. Let C^n be a cycle on M'_i mod K_i and let $M''_i \subset M'_i$ be a minimal locus of concentration for the cycle C^n, that is, M''_i is a closed set such that every open set $\supset M''_i$ is a carrier of C^n and M''_i is minimal with respect to that property. The existence of such a minimal locus of concentration is guaranteed by [**2**, p. 205, 2.2]. Let x be a point on the boundary of M''_i relative to M_i; such points exist since M_i is connected and M''_i is a proper closed subset, and $x \in M''_i$. Since $p_n(M_i \bmod K_i, x) = 1$, there exist open sets V, U such that $x \in V$, $\bar{V} \subset U$, and such that there is only one n-cycle on M_i mod $[(M_i - U) \cup K_i]$ linearly independent with respect to homologies mod $[(M_i - V) \cup K_i]$. Now both C^n and $z^n{}_i$ are cycles mod K_i, hence, mod $[(M_i - U) \cup K_i]$; therefore, there exist elements a_1 and a_2 of the coefficient field, not both zero, such that

$$a_1 z^n{}_i + a_2 C^n \sim 0 \mod [(M_i - V) \cup K_i].$$

Now $z^n{}_i$ is not $\backsim 0$ mod $[(M_i - V) \cup K_i]$, for if it were, then it would be equal to zero on $V - K_i$ (since only n-dimensional coverings are being used), and $z^n{}_i$ would be on the proper closed subset $(M - V) \cup K_i$ of M_i, contrary to the orientability of M_i. Also if $M''_i \not\subset K_i$ then C^n is not $\backsim 0$ mod $[(M_i - V) \cup K_i]$ for if it were, then, as above,

$$[(M_i - V) \cup K_i] \cap M''_i$$

would be a proper closed subset of M''_i and a locus of concentration for C^n, contrary to the minimal property of M''_i. We therefore conclude that $a_1 \neq 0$ and $a_2 \neq 0$ in the preceding homology, and that

$$C^n \sim -(a_1/a_2) z^n_i \mod [(M_i - V) \cup K_i] \text{ on } M_i;$$

hence $z^n = -(a_1/a_2) z^n{}_i$ on $V - K_i$. Since x is a boundary point of M''_i and $K_i = \bar{A}_i - A_i$, there is a point $y \in V - K_i - M''_i$. Let W be an open set such that

$$x \in W, \quad \bar{W} \cap M''_i = 0, \quad W \subset V - K_i - M''_i.$$

Now just as before $z^n{}_i \neq 0$ on W, but $C^n = 0$ on W, since M''_i is a locus of concentration and this requires the open set $M_i - \bar{W} \supset M''_i$ to carry C^n. This is, however, contrary to $C^n = -(a_1/a_2) z^n{}_i$ on $V - K_i$; therefore we conclude that $M''_i \subset K_i$, and that $C^n = 0$ mod K_i.

COROLLARY 3.1.1. *A necessary and sufficient condition that the* n-gm M *with boundary* K *be orientable is that* $p^n(M_i, K_i) = 1$ *for each component* M_i *of* M *where* $K_i = K \cap M_i$, *and that each* M_i *satisfy condition* D; *in particular, a*

necessary and sufficient condition that a connected n-gm M *with boundary* K *be orientable is that* $p^n(M, K) = 1$, *and* M *satisfy* D.

Proof. The necessity follows from Theorems 2.4 and 3.1. The sufficiency follows from Theorem 2.4 which requires each M_t to be orientable, and from the fact that M is clearly orientable if each component is.

COROLLARY 3.1.2. *If* M *is an orientable* n-gm *with boundary* K, *then* $p^n(M, K)$ *is the number of components of* M.

Proof. By Corollary 3.1.1, $p^n(M_t, K_t) = 1$ for each component; therefore $p^n(M, K)$ is the number of components, since $H^n(M, K)$ is isomorphic to the direct sum of the groups $H^n(M_t, K_t)$.

COROLLARY 3.1.3. *A necessary and sufficient condition that an orientable* n-gm M with boundary K *be an* n-D-gm *is that* M *be connected.*

Proof. The necessity follows from Corollary 3.1.2 and Theorem 2.4. The sufficiency follows directly from the Theorem.

The above theorem and corollaries allow us to restrict our attention in the orientable case to the n-D-gm.

THEOREM 3.2. *If* M *is an orientable* n-D-gm (*or equivalently connected orientable* n-gm) *with boundary* K, *then* M *is an irreducible membrane relative ro* z^{n-1}, *the cycle referred to in the Definition* 2.1. (See Definition [**2**, p. 209].)

Proof. In the proof of Theorem 2.2 it was shown that if z^n is the cycle on M mod K in Definition 2.1, then $\partial z^n = z^{n-1}$ satisfies the definition of orientability for the $(n-1)$-gcm K. Clearly $z^{n-1} \backsim 0$ on M; suppose also that $z^{n-1} \backsim 0$ on M_1, a proper closed subset of M. By [**2**, p. 201, Lemma 1.4] there exists a cycle $z^n{}_1$ on M_1 mod K such that $\partial z^n{}_1 \backsim z^{n-1}$ on K. Thus

$$\partial(z^n - z^n{}_1) = z^{n-1} - \partial z^n{}_1 \sim 0 \text{ on } K$$

and by [**2**, p. 201, Lemma 1.6] there exists a cycle C^n on M such that $z^n - z^n{}_1 \backsim C^n$ on M mod K. By property D, $C^n \backsim 0$; hence $z^n \backsim z^n{}_1$ mod K on M contrary to the orientability hypothesis of M. Thus M is an irreducible membrane for the homology $z^{n-1} \backsim 0$ on M.

Definition 3.1. If K is a closed subset of the compact space M then $g^r(M; K, 0)$ is the maximum number of r-cycles on $K \backsim 0$ on M and linearly independent with respect to homologies on K [**2**, p. 211].

THEOREM 3.3. *If* M *is an orientable* n-D-gm *with boundary* K, *then* $g^{n-1}(M; K, 0) = 1$ *irreducibly* (that is, $g^{n-1}(M; K, 0) = 1$ *and* $g^{n-1}(M; K_1, 0) = 0$ *where* K_1 *is a proper closed subset of* K).

Proof. Theorem 3.2 yields a cycle z^{n-1} on $K \backsim 0$ on M such that $z^{n-1} \nsim 0$ on K (since $z^{n-1} \sim 0$ on any proper closed subset of M). Thus $g^{n-1}(M; K, 0) \geqslant 1$. Now consider two cycles $z^{n-1}{}_1$ and $z^{n-1}{}_2$ on K such that $z^{n-1}{}_i \backsim 0$ on M $(i = 1, 2)$.

By [2, p. 201, Lemma 1.4], there exist cycles C^n_i on M mod K such that $\partial C^n_i \backsim z^{n-1}_i$ on K $(i = 1, 2)$. By Theorem 8, $p^n(M, K) = 1$; hence there exist elements a_1, a_2 of the coefficient field, not both zero, such that $a_1C^n_1 + a_2C^n_2 \backsim 0$ on M mod K. By [2, p. 201, Lemma 1.3],

$$\partial(a_1C^n_1 + a_2C^n_2) = a_1\partial C^n_1 + a_2\partial C^n_2 \sim 0 \text{ on } K;$$

hence $a_1z^{n-1}_1 + a_2z^{n-1}_2 \backsim 0$ on K, that is, $g^{n-1}(M; K, 0) \leqslant 1$. Thus $g^{n-1}(M; K, 0) = 1$.

Next consider the proper closed subset K_1 of K and a cycle z^{n-1}_1 on K_1 such that $z^{n-1}_1 \backsim 0$ on M. As before, there exists a cycle C^n_1 on M mod K_1 such that $\partial C^n_1 \backsim z^{n-1}_1$ on K_1. By Theorem 4, $p^n(M, K_1) = 0$; hence $C^n_1 \backsim 0$ on M mod K_1, which implies that $z^{n-1}_1 \backsim 0$ on K_1. Thus $g^{n-1}(M; K_1, 0) = 0$.

4. The generalized n-cell. Before proving the next theorem we prove three lemmas needed later.

LEMMA 1. *If M is an n-gm with boundary K, then $A = M - K$ is* ulc^{n-1} (uniformly r-locally connected $r \leqslant n - 1$).

Proof. Let A' be homeomorphic with A such that $A' \cap A = 0$ and such that $A' \cup K$ is an n-gm M' with boundary K; then by Theorem 2.4 of (1) $M \cup M' = S$ is an n-gcm. By [2, p. 292, Theorem 1.7] we have $S - K = A' \cup A$ is $(n - r - 1)$ − ulc for $0 \leqslant n - r - 1 \leqslant n - 1$, since

$$p_r(K, x) = p^r(K, x) = 0, \qquad 0 \leqslant r \leqslant n - 1,$$

by Theorem 1.2. Since A' and A are separate, this implies that A is ulc^{n-1}.

LEMMA 2. *If M is an orientable n-gm with boundary K and γ^r, $r \leqslant n - 1$, is a cycle on K, then there exists a compact cycle z^r in $A = M - K$ such that $\gamma^r \backsim z^r$ on M.*

Proof. As in the preceding proof an n-gcm S can be constructed with A as an open ulc^{n-1} subset of S. Furthermore it follows from Theorem 3.2 of (1) that S is orientable. The conclusion now follows from [2, p. 301, Theorem 5.9].

LEMMA 3. *If M is an orientable n-gm with boundary K such that $A = M - K$ is an F_σ, then $h^{n-r}(A) \approx H^r(M, K)$ $r \leqslant n$ if either group has finite dimension,* where $h^s(A)$ denotes the s-dimensional (unaugmented) homology group of A with respect to compact cycles.

Proof. As in the preceding lemmas, A can be considered as an open subset of an n-gcm. By Theorem 2.1, A is an orientable non-compact n-gm. By [2, p. 258, Theorems 5.13 and 5.14], $H^r(A) \approx h^{n-r}(A)$, $r \leqslant n$, if either group has finite dimension, where $H^r(A)$ is the r-dimensional homology group of A with respect to infinite cycles. By the remark after Theorem 1.3, $H^r(A) \approx H^r(M, K)$; thus $h^{n-r}(A) \approx H^r(M, K)$, $r \leqslant n$.

Definition 4.1. *A generalized closed n-cell* is an orientable n-D-gm with a non-vacuous boundary K such that $p^r(M, K) = 0$, $0 < r < n$.

THEOREM 4.1. *If K is a closed subset of M such that $M - K$ is an F_σ, then a necessary and sufficient condition that M be a generalized closed n-cell with boundary K is that*:

(1) $M = K \cup A$, $K \cap A = 0$, dim $M = n$.

(2) *K is an* $(n-1)$-gcm.

(3) *A is a generalized* (open) *n-cell* (i.e., a non-compact orientable n-gm satisfying D′ which is cell-like in the sense that its compact (augmented) homology groups of dimensional $< n$ reduce to the identity).

(4) $p_r(M, x) = 0, r \leqslant n$, *for all* $x \in K$.

Proof of necessity. By Theorems 1.3 and 2.1, it follows that (1), (2), (4) are satisfied, and that A is an orientable n-gm satisfying D′. By Theorem 2.3, $p^n(M, K) = 1$, and by hypothesis $p^r(M, K) = 0$, $0 < r < n$; therefore by Lemma 13.3,

$$h^{n-r}(A) \approx H^r(M, K), \qquad 0 < r \leqslant n.$$

Thus for $0 < r < n$, $h^{n-r}(A) \approx 0$ and $h^0(A)$ has dimension 1, or if the augmented homology groups are used the 0-dimensional group also reduces to the identity, as required in condition (3).

Proof of sufficiency. M is an orientable n-D-gm by Theorems 1.3 and 2.1. By Lemma 13.3 $h^{n-r}(A) \approx H^r(M, K)$ for $0 \leqslant n - r < n$, i.e., for $0 < r \leqslant n$ since the dimension of the left-hand group is finite by property (3). In particular, $h^{n-r}(A) \approx 0$ for $0 < n - r < n$; therefore $p^r(M, K) = 0$ for $0 < r < n$.

THEOREM 4.2. *If M is a generalized closed n-cell with boundary K, such that $A = M - K$ is an F_σ, then $p^r(M) = 0$ for all r* (where augmented theory is used).

Proof. By Corollary 3.1.3, M is connected and $p^r(M) = 0$ (using augmented theory). Next let z^r be a cycle on M, $0 < r < n$. Since z^r is also a cycle mod K and $p^r(M, K) = 0$, $0 < r < n$, it follows that $z^r \backsim 0$ mod K on M. By [**2**, p. 203, Lemma 1.13], there is a cycle γ^r on K such that $\gamma^r \backsim z^r$ on M. By Lemma 2 above, there is a compact cycle C^r of A such that $\gamma^r \backsim C^r$ on M. Since by Theorem 4.1, A is a generalized n-cell, $C^r \backsim 0$ on A; hence, $z^r \backsim 0$ on M. Since M is an n-D-gm,

$$p^n(M, 0) = p^n(M) = 0$$

by Theorem 4. Finally, $p^r(M) = 0$ for all $r > n$ since M is n-dimensional; thus $p^r(M) = 0$ for all r.

THEOREM 4.3. *If M is a generalized closed n-cell with boundary K, such that $A = M - K$ is an F_σ, then K is a sphere-like* $(n-1)$-gcm. (The $(n-1)$-gcm is sphere-like if its homology groups are isomorphic to those of the $(n-1)$-sphere.)

Proof. Let z^r, $0 \leqslant r \leqslant n - 2$, be a cycle on K, then by Lemma 2 above, there is a compact cycle γ^r in A such that $z^r \backsim \gamma^r$ on M. By Theorem 4.1, A is a generalized n-cell, and it follows that $\gamma^r \backsim 0$ in A; hence $z^r \backsim 0$ on M. By

[2, p. 201, Lemma 1.4], there is a cycle C^{r+1} mod K on M such that $\partial C^{r+1} \frown z^r$ on K. Now $1 \leqslant r+1 \leqslant n-1$; hence $p^{r+1}(M, K) = 0$, by hypothesis. Thus $C^{r+1} \frown 0$ mod K on M, and by [2, p. 201, Lemma 1.3], $z^r \frown 0$ on K. By Theorem 2.2, K is orientable; therefore, there is at least one cycle z^{n-1} on K, not $\frown 0$ on K; hence $p^{n-1}(K) > 0$. Consider two cycles $z^{n-1}{}_1$ and $z^{n-1}{}_2$ on K, then by the same argument used above in the lower dimensions, we have two cycles $C^n{}_1$ and $C^n{}_2$ mod K on M such that $\partial C^n{}_i \frown z^{n-1}{}_i$ on K $(i = 1, 2)$. Since M is an orientable n-D-gm, we have $p^n(M, K) = 1$ by Theorem 2.3; therefore, there exist elements a_1 and a_2 of the coefficient group, not both 0, such that

$$a_1 C^n{}_1 + a_2 C^n{}_2 \sim 0 \mod K \text{ on } M.$$

Thus as before $a_1 \partial C^n{}_1 + a_2 \partial C^n{}_2 \frown 0$ on K; hence,

$$a_1 z^{n-1}{}_1 + a_2 z^{n-1}{}_2 \sim 0 \text{ on } K,$$

which proves that $p^{n-1}(K) = 1$.

THEOREM 4.4. *If M is a generalized closed n-cell with boundary K, such that $A = M - K$ is an F_σ, and if z^{n-1} is a non-bounding $(n-1)$-cycle on K, then M is an irreducible membrane relative to z^{n-1}.*

Proof. By Theorem 3.2 there is one cycle z^{n-1} on K satisfying the conclusion of the theorem. By Theorem 4.3 any two non-bounding $(n-1)$-cycle on K are linearly dependent; therefore, any such cycle satisfies the conclusion of the theorem.

Remark. Wilder has defined a generalized closed n-cell [2, p. 287] as a compact space M satisfying Conditions (1), (2), (3), and (4) of Theorem 4.1, and in addition the properties in the conclusions of Theorems 4.3 and 4.4. Thus we have proved (at least in the case where $M - K$ is on F_σ), that the weakened conditions (1), (2), (3), and (4) are equivalent to Wilder's apparently stronger conditions. It should also be noted that if (1), (2), (3), and (4) are taken as the definition of a closed n-cell, then an examination of the proofs of Theorems 4.2, 4.3, and 4.4 shows that the conclusions of those theorems hold without the hypothesis that $M - K$ be an F_σ if the additional assumption $p^r(M, K) = 0$, $0 < r < n$, is added. Thus we have proved the following theorem.

THEOREM 4.5. *A necessary and sufficient condition that the n-gm M with boundary K, such that $A = M - K$ is an F_σ, be a generalized closed n-cell in the sense of Wilder is that $p^r(M, K) = 0$, $0 < r < n$, or that A be a generalized* (open) *n-cell.*

The next theorem, which is a summary of the necessary and sufficient conditions contained in Theorems 1.2, 1.3, 2.1, and 4.1, shows that in each case the condition imposed on M is equivalent to a similar condition on $A = M - K$ in the presence of three other conditions that do not change.

THEOREM 4.6. *A necessary and sufficient condition that M be*:

(a) *an n-gm with boundary,*

(b) *an n-D-gm with boundary,*

(c) *an orientable n-gm with boundary,*

(d) *a generalized closed n-cell,*

is that there exists a closed subset K of M, such that:

(1) $M = K \cup A$, $K \cap A = 0$, $\dim M = n$.

(2) *K is an $(n-1)$-gcm.*

(3) *A is an open, non-compact* { (a) *n-gm,* (b) *n-gm satisfying* D′, (c) *orientable n-gm,* (d) *generalized n-cell.*

(4) $p_r(M, x) = 0$, $r \leqslant n$, *for all* $x \in K$.

(In case (d) the additional hypothesis that A be an F_σ must be included.)

5. Classical manifolds. We close with two theorems which show that the generalized manifolds with boundary reduce to the classical ones in the one- and two-dimensional separable cases.

THEOREM 5.1. *If M is a connected, separable* 1-gm *with boundary K and $K = 0$, then M is a* 1*-sphere and if $K \neq 0$, then M is an arc with end points a and b such that $K = a \cup b$.*

Proof. By Theorem 1.2, K is a 0-gcm, that is, a finite set of points; and by Conditions (2) and (4), M is a Peano continuum. Suppose M is not a 1-sphere; then either M is acyclic or contains a 1-sphere J. If $M \supset J$, but $M \neq J$, then the argument in the remarks on [2, p. 271] yields a neighbourhood P of a point $x \in J$ and three arcs xx', xy', and xy such that each lies entirely in P except their end points x', y', and y which lie on the boundary of P, and each pair of arcs has only the point x in common. We can also suppose P is chosen so that it contains no points of $K - x$. Then the arcs $(x'x \cup xy)$ and $(x'x \cup xy')$ carry 1-cycles mod $[(M - \mathrm{P}) \cup K]$ (actually mod $(M - P)$) which, because M is one-dimensional, are linearly independent with respect to homologies mod $[(S - Q) \cup K]$ for every $Q, \bar{Q} \subset P$, contrary to $p_1(M \bmod K; x) = 1$. If M is acylic, then $M \supset$ a (maximal) non-degenerate arc J. If $M \neq J$, the argument above again yields a neighbourhood P of an interior point $x \in J$ and three arcs xx', xy', and xy with the above properties, and leads to a contradiction as before. Thus M is either a 1-sphere or an arc. If M is a 1-sphere, then $K = 0$; for if $x \in K$, then

$$p_1(M \bmod K; x) = p_1(M \bmod x; x) = 2,$$

contrary to property (3). If M is an arc with end points a and b, then $K \subset a \cup b$ by the argument just applied above for the 1-sphere. Finally $a, b \in K$, for if $a \notin K$ then

$$p_1(M \bmod K, a) = p_1(M, a) = 0,$$

contrary to property (3). This shows that the remainder of the theorem holds.

COROLLARY 5.1. *If M is a separable* 1-gm *with boundary K, then M consists of a finite number of components each of which is a* 1*-sphere or an arc.*

Proof. This follows directly from Theorem 5.1 and the fiirst part of Theorem 3.1.

THEOREM 5.2. *If M is a connected separable* 2-gm *with boundary K, then M is a classical* 2-gm *from which a finite number of open* 2*-cells whose closures are disjoint have been deleted. K consists of the union of the* 1*-spheres that form the boundaries of the deleted* 2*-cells.*

Proof. By Theorem 1.2, K is a 1-gcm, hence $K = J_1 \cup J_2 \cup \ldots \cup J_k$, where the (J_i) are pairwise disjoint 1-spheres. Let

$$M' = (A_1 \cup J_1) \cup (A_2 \cup J_2) \cup \ldots \cup (A_k \cup J_k)$$

where each A_i is an open 2-cell with boundary J_i, $A_i \cap A_j = 0$, $i \neq j$, and $A_i \cap M = 0$ for all i. Now M' is a 2-gm with boundary K and by (1) $M' \cup M$ is a 2-gm. By [**2**, p. 272, Theorem 2.3], $M' \cup M$ is a classical 2-gcm and our theorem follows. (If M is not assumed connected then as before M consists of a finite number of components each of which has the property of Theorem 5.2.)

REFERENCES

1. P. A. White, *On the union of two generalized manifolds*, Scuola Normale Superiore (1950).
2. R. L. Wilder, *Topology of manifolds* (American Mathematical Society Colloquium Publications, vol. 32, 1949).

University of Southern California

ON THE NUMBER OF SOLUTIONS OF SOME GENERAL TYPES OF EQUATIONS IN A FINITE FIELD

OLIN B. FAIRCLOTH

1. **Introduction.** The conditional equation $f(x_1, \ldots, x_s) = 0$, where f is a polynomial in the x's with coefficients in a finite field $F(p^n)$, is connected with many well-known developments in number theory and algebra, such as: Waring's problem, the arithmetical theory of quadratic forms, the Riemann hypothesis for function fields, Fermat's Last Theorem, cyclotomy, and the theory of congruences in commutative rings.

In this paper we shall investigate *the number of distinct solutions, N_s, of equations of the type*

$$c_1x_1^{m_1} + c_2x_2^{m_2} + \ldots + c_sx_s^{m_s} = c, \tag{1.1}$$

$s \geqslant 2$, where the c's are given elements of a finite field $F(p^n)$, $c_1 \ldots c_s \neq 0$, p is an odd prime, and $p^n - 1 = q_im_i$ for each i. If $c \neq 0$, we shall for convenience consider the equation

$$g^{y_1m_1+r_1} + \ldots + g^{y_sm_s+r_s} = 1, \tag{1.2}$$

where g is a multiplicative generator of $F(p^n)$ aside from zero and

$$\frac{c_i}{c} = g^{km_i+r_i}.$$

Let $(r_1, \ldots, r_s)$ denote the number of distinct sets of y's $(y_i = 0, 1, \ldots, q_i - 1)$ that satisfy (1.2); thus $(r_1, \ldots, r_s)\, m_1 \ldots m_s$ is the number of non-zero solutions of (1.1).

If α_i is a primitive m_i root of unity and ind a is defined such that $g^{\text{ind } a} = a$ for any non-zero a in $F(p^n)$, consider the generalized Jacobi-Cauchy cyclotomic sum

$$\psi(u_1, \ldots, u_s) = \sum_{a_1+\ldots+a_s=1} \prod_{i=1}^{s} \alpha_i^{u_i \text{ ind } a_i}, \tag{1.3}$$

where the a's range over the non-zero elements of $F(p^n)$. Vandiver [7, p. 148] in a recent paper gave the following expression for the number of non-zero solutions of (1.1):

$$(r_1, \ldots, r_s) \prod_{i=1}^{s} m_i = \sum_{u_1,\ldots,u_s} \psi(u_1, \ldots, u_s) \prod_{i=1}^{s} \alpha_i^{-u_ir_i}, \tag{1.4}$$

where each u_i ranges independently over the set $0, 1, \ldots, m_i - 1$.

2. Additive decomposition formulae for $(r_1, \ldots, r_s)$. In order to apply these sums to the aforementioned equation, we shall first consider degenerate cases. If $u_i \equiv 0 \pmod{m_i}$ for each i, then

Received March 12, 1951; in revised form October 23, 1951.

$$\psi(0, \ldots, 0) = \sum_{a_1+\ldots+a_s=1} 1.$$

Our problem reduces to counting the sets of a's for which $a_1 + \ldots + a_s = 1$. This number is easily obtained by induction and we have

LEMMA 2.1. *If $u_i \equiv 0 \pmod{m_i}$ for each i, then*

$$\psi(0, \ldots, 0) = \{(p^n - 1)^s - (-1)^s\}/p^n.$$

This result was found independently by Whiteman [9].

Suppose $u_1 \equiv 0 \pmod{m_1}$ and $u_s \not\equiv 0 \pmod{m_s}$; we then have

$$\psi(0, u_2, \ldots, u_s) = \sum_{a_1+\ldots+a_s=1} \prod_{i=2}^{s} a_i^{u_i \text{ ind } a_i}.$$

In the above sum $a_2, \ldots, a_s$ range independently over all the non-zero elements of $F(p^n)$ except those for which $a_2 + \ldots + a_s = 1$; thus $\psi(0, u_2, \ldots, u_s) = -\psi(u_2, \ldots, u_s)$. By continually applying this result we obtain

LEMMA 2.2. *If $u_i \equiv 0 \pmod{m_i}$, $i = 1, \ldots, t$, $t < s$, and $u_s \not\equiv 0 \pmod{m_s}$, then*

$$\psi(0, \ldots, 0, u_{t+1}, \ldots, u_s) = (-1)^t \psi(u_{t+1}, \ldots, u_s).$$

As our last degenerate case suppose

$$\prod_{i=1}^{s} a_i^{u_i} = 1, \qquad u_s \not\equiv 0 \pmod{m_s}.$$

Under this assumption (1.3) may be written

$$\psi(u_1, \ldots, u_s) = \sum_{a_1+\ldots+a_s=1} \prod_{i=2}^{s} a_i^{u_i \text{ ind } a_i/a_1}. \tag{2.1}$$

Let $a_i = -b_i a_1$, $i > 1$; the right-hand side of (2.1) becomes

$$\sum_{a_1(1-b_2-\ldots-b_s)=1} \prod_{i=2}^{s} a_i^{u_i \text{ ind } b_i} a_1^{u_i \text{ ind } (-1)}.$$

In the above sum $b_2, \ldots, b_s$ range independently over the non-zero elements of $F(p^n)$ except those for which $1 - b_2 - \ldots - b_s = 0$. Thus we have

LEMMA 2.3. *If*

$$\prod_{i=1}^{s} a_i^{u_i} = 1, \qquad u_s \not\equiv 0 \pmod{m_s},$$

then

$$\psi(u_1, \ldots, u_s) = -\psi(u_2, \ldots, u_s) a_1^{u_1 \text{ ind } (-1)}.$$

Lemma 2.1 and Lemma 2.2 enable us to write the right-hand side of (1.4) as sums of ψ's where none of the u's are zero. Let

$$\Phi(r_1, \ldots, r_t) = \sum_{u_1, \ldots, u_t} \psi(u_1, \ldots, u_t) \prod_{i=1}^{t} a_i^{-u_i r_i}, \tag{2.2}$$

where each u_i ranges independently over the set $1, \ldots, m_i - 1$. From Lemma 2.3 we have, in the case $t > 2$,

$$\Phi(r_1, \ldots, r_s) = \sum \psi(u_1, \ldots, u_t) \prod_{i=1}^{t} a_i^{-u_i r_i} - \sum \psi(u_2, \ldots, u_t) a_1^{u_1 \operatorname{ind}(-1)} \prod_{i=1}^{t} a_i^{-u_i r_i}, \tag{2.3}$$

where in the first sum each u_i ranges over the set $1, \ldots, m_i - 1$ such that

$$\prod_{i=1}^{t} a_i^{u_i} \not\equiv 1,$$

and in the second sum each u_i ranges over the set $1, \ldots, m_i - 1$ such that

$$\prod_{i=1}^{t} a_i^{u_i} = 1.$$

If F is an arbitrary function of the b's then denote by

$$\sum_{t}^{s} F(b_1, \ldots, b_t) \tag{2.4}$$

the sum of the F's of the $\binom{s}{t}$ distinct sets of b's taken t at a time. If we expand the right-hand side of (1.4) and reduce the degenerate terms by Lemmas 2.1 and 2.2, we have

THEOREM 2.1.

$$(r_1, \ldots, r_s) \prod_{i=1}^{s} m_i = \{(p^n - 1)^s - (-1)^s\}/p^n + \sum_{t=1}^{s} (-1)^{s-t} \sum_{t}^{s} \Phi(r_1, \ldots, r_t),$$

where $\Phi(r_1, \ldots, r_t)$ *is defined by* (2.3).

Theorem 2.1 enables us in special cases to find the exact values of

$$(r_1, \ldots, r_s) \prod_{i=1}^{s} m_i$$

in terms of p, n, and m's explicitly. As an example, suppose $m_1 = \ldots = m_s = m$, n even and $p^{\frac{1}{2}n} + 1 \equiv 0 \pmod{m}$. If $u_i \not\equiv 0 \pmod{m}$ for any i and

$$\psi_{j,t} = \psi(u_1 + \ldots + u_j, u_{j+1}, \ldots, u_t),$$

then

$$\psi_{1,t} = p^{kn} \psi_{1,2} \psi_{2,3} \cdots \psi_{t-1,t}, \tag{2.5}$$

where k is the number of j's for which $u_1 + \ldots + u_j \equiv 0 \pmod{m}$, $j < t$. (For proof see [1, p. 265].) If $u_1 + \ldots + u_j \equiv 0 \pmod{m}$, we have from Lemmas 2.2 and 2.3,

$$\psi_{j-1,j} = \psi_{j,j+1} = -1.$$

If $u_1 + \ldots + u_j \not\equiv 0 \pmod{m}$, Mitchell [5, p. 177] proved $\psi_{j-1,j} = p^{\frac{1}{2}n}$. Among the first $t - 2$ elements in the right-hand side of (2.5), $2k$ have the value -1 and the remaining have the value $p^{\frac{1}{2}n}$; thus

$$\psi_{1,t} = \begin{cases} p^{\frac{1}{2}n(t-1)}, & u_1 + \ldots + u_t \not\equiv 0 \pmod{m}, \\ -p^{\frac{1}{2}n(t-2)}, & u_1 + \ldots + u_t \equiv 0 \pmod{m}. \end{cases}$$

As the u's range independently over the set $1, 2, \ldots, m-1$, we have, by an easy induction, $u_1 + \ldots + u_t \not\equiv 0 \pmod{m}$ for $(m-1\{(m-1)^t - (-1)^t\}/m$ sets of u's, and $u_1 + \ldots + u_t \equiv 0 \pmod{m}$ for $(m-1)\{(m-1)^{t-1} - (-1)^{t-1}\}/m$ sets of u's. Thus if $r_1 \equiv \ldots \equiv r_s \equiv 0 \pmod{m}$,

$$\Phi(r_1, \ldots, r_t) = p^{ln(t-1)}(m-1)\{(m-1)^s - (-1)^s - p^{-ln}((m-1)^{t-1} + (-1)^t)\}/m.$$

If we substitute this value in Theorem 2.1 and reduce the resulting sum, we obtain

$$N = (p^n - 1)^s/p^n + \{(mp^{ln} - p^{ln} - 1)^{s+1} + (m-1)(-p^{ln} - 1)^{s+1}\}/mp^n. \tag{2.6}$$

In the above formula N denotes the number of non-zero solutions in $F(p^n)$ (n even and $p^{ln} + 1 \equiv 0 \pmod{m}$) of

$$x_1^m + \ldots + x_s^m = 1.$$

We shall now obtain another additive decomposition formula for $(r_1, \ldots, r_s)$. Suppose for any $t < k > 2$,

$$(r_1, \ldots, r_t)\prod_{i=1}^{t} m_i = p^{(t-1)n} - \sum_{j=1}^{t-1} \sum_{j}^{t} (r_1, \ldots, r_j)\prod_{i=1}^{j} m_i + \Phi(r_1, \ldots, r_t). \tag{2.7}$$

This is obviously true for $k = 2$. If we solve for $\Phi(r_1, \ldots, r_t)$ in (2.7) and substitute in Theorem 2.1, $s = k+1$, we have

$$(r_1, \ldots, r_{k+1})\prod_{i=1}^{k+1} = \{(p^n - 1)^{k+1} - (-1)^{k+1}\}/p^n + \sum_{t=1}^{k} (-1)^{k+1-t} \sum_{t}^{k+1} \{-p^{(t-1)n} + \sum_{j=1}^{t} \sum_{j}^{t} (r_1, \ldots, r_j)\prod_{i=1}^{j} m_i\} + \Phi(r_1, \ldots, r_{k+1}).$$

For any $t > j$ we note that the term $(r_1, \ldots, r_j)$ will be contained in the remaining $k+1-j$ sets taken $t-j$ at a time; thus the coefficient of

$$(r_1, \ldots, r_j)\prod_{i=1}^{j} m_i$$

is

$$\sum_{t=j}^{k} (-1)^{k+1-t}\binom{k+1-j}{t-j},$$

which can be reduced to minus one. The constant terms, when collected, are

$$\frac{(p^n - 1)^{k+1} - (-1)^{k+1}}{p^n} - \sum_{t=1}^{k} (-1)^{k+1-t}\binom{k+1}{t} p^{(t-1)n},$$

which can be reduced, in a similar manner, to p^{kn}. Thus we have established by induction

THEOREM 2.2. *If* $s \geqslant 2$,

$$(r_1, \ldots, r_s) \prod_{i=1}^{s} m_i = p^{(s-1)n} - \sum_{t=1}^{s-1} \sum_{t}^{s} (r_1, \ldots, r_t) \prod_{i=1}^{t} m_i + \Phi(r_1, \ldots, r_s),$$

where Φ *is defined in* (2.3).

If $c \not\equiv 0$ in equation (1.1),

$$N_s = \sum_{t=1}^{s} \sum_{t}^{s} (r_1, \ldots, r_t) \prod_{i=1}^{t} m_i;$$

thus we immediately obtain from Theorem 2.2 the

COROLLARY. $\qquad N_s = p^{(s-1)n} + \Phi(r_1, \ldots, r_s).$

Weil [8, p. 502] has a more complicated expression for N_s in terms of characters.

If $u_t \not\equiv 0 \pmod{m_t}$ for any i,

$$|\psi(u_1, \ldots, u_s)| = \begin{cases} p^{\frac{1}{2}n(s-1)}, & \prod_{i=1}^{s} a_i^{u_i} \neq 1, \\ p^{\frac{1}{2}n(s-2)}, & \prod_{i=1}^{s} a_i^{u_i} = 1. \end{cases}$$

(For proof see [1, p. 263].) From the Corollary we then obtain

$$|N_s - p^{(s-1)n}| \leqslant p^{\frac{1}{2}n(s-1)} \left(\prod_{i=1}^{s} (m_i - 1) - K_s \right) + p^{\frac{1}{2}n(s-2)} K_s,$$

where K_s is the number of sets of u's for which

$$\prod_{i=1}^{s} a_i^{u_i} = 1.$$

This limit is better than that given by Hua and Vandiver [2, p. 99] or Weil [8, p. 502]. Whiteman [9, p. 378] found that

$$K_s = \sum_{t=2}^{s} (-1)^{s-t} \sum_{t}^{s} \frac{m_1 \ldots m_t}{[m_1, \ldots, m_t]} + (-1)^{s-1}(s-1),$$

where $[m_1, \ldots, m_t]$ is the least common multiple of $m_1, \ldots, m_t$.

We can again give the exact values of N_s in certain special cases.

3. Linear relations involving $(r_1, \ldots, r_s)$. If in relation (1.4) we let r_t range over the set $0, 1, \ldots, m_t - 1$ $(i = 1, \ldots, t)$, we have for $t < s$,

$$\sum_{r_1, \ldots, r_t} (r_1, \ldots, r_s) \prod_{i=1}^{s} m_i \tag{3.1}$$

$$= \sum_{u_1, \ldots, u_s} \psi(u_1, \ldots, u_s) \prod_{i=t+1}^{s} a_i^{-u_i r_i} \sum_{r_1, \ldots, r_t} \prod_{i=1}^{t} a_i^{-u_i r_i}.$$

We see that each term equals zero unless $u_t = 0$ for each i $(i = 1, \ldots, t)$; thus the right-hand side of (3.1) becomes

$$\prod_{i=1}^{t} m_i \sum_{u_{t+1}, \ldots, u_s} \psi(0, \ldots, 0, u_{t+1}, \ldots, u_s) \prod_{i=t+1}^{s} a_i^{-u_i r_i}.$$

$\psi(0, \ldots, 0, u_{t+1}, \ldots, u_s)$ can be reduced by Lemma 2.2 if $u_i \neq 0$ for some i. If we add and subtract $\psi(u_{t+1}, \ldots, u_s)$, $u_{t+1} = \ldots = u_s = 0$, we obtain

$$\sum_{r_1,\ldots,r_s} (r_1, \ldots, r_s) \prod_{i=t+1}^{s} m_i = \{(p^n - 1)^s - (-1)^s\}/p^n$$

$$- (-1)^t\{(p^n - 1)^{s-t} - (-1)^{s-t}\}/p^n + (-1)^t \sum \psi(u_{t+1}, \ldots, u_s) \prod_{i=t+1}^{s} a_i^{-u_i r_i},$$

where each u_i ranges independently over the set $0, 1, \ldots, m_i - 1$; thus we have, in view of (1.4),

THEOREM 3.1.

$$\sum_{r_1,\ldots,r_s} (r_1, \ldots, r_s) \prod_{i=t+1}^{s} m_i = (p^n - 1)^{s-t}\{(p^n - 1)^t - (-1)^t\}/p^n$$

$$+ (-1)^t (r_{t+1}, \ldots, r_s) \prod_{i=t+1}^{s} m_i,$$

where for $i = 1, \ldots, t$ $(t < s)$, each r_i ranges independently over the set $0, 1, \ldots, m_i - 1$.

4. On equation (1.1) with $c = 0$. In this section we shall investigate the number of distinct non-zero solutions of equation (1.1) with $c = 0$. With a slight modification of the function defined in (1.3) we can establish relations analogous to those given in Theorem 2.1 and Theorem 2.2 for this case. Owing to the special character of this problem we are able to find by elementary methods a recursion formula that expresses the number of solutions of (1.1) in terms of the number of solutions of equations containing fewer terms. The methods employed here first appeared in a paper by Hua and Vandiver [4, p. 486].

If the m's in (1.1) are grouped into k sets which are prime each to each, we have an equation of the form

$$\sum_{i=1}^{s_1} c_{1,i} x_{1,i}^{m_{1,i}} + \ldots + \sum_{i=1}^{s_k} c_{k,i} x_{k,i}^{m_{k,i}} = 0. \tag{4.1}$$

Let m_j be the least common multiple of $m_{j,i}$ for each j and $i = 1, \ldots, s_j$; thus $(m_h, m_t) = 1$, $h \neq t$. Also impose the condition that $m_j = m_{j,1}$ for each j less than k. *Denote by $N_{t,k}$ the number of non-zero solutions of*

$$\sum_{i=1}^{s_t} c_{t,i} x_{t,i}^{m_{t,i}} + \ldots + \sum_{i=1}^{s_k} c_{k,i} x_{k,i}^{m_{k,i}} = 0. \tag{4.2}$$

Also denote by H_t and G_t the number of distinct non-zero solutions of

$$h_t \equiv \sum_{i=1}^{s_t} c_{t,i} x_{t,i}^{m_{t,i}} = 0 \tag{4.3}$$

and

$$g_t \equiv c_{t,1} + \sum_{i=2}^{s_t} c_{t,i} x_{t,i}^{m_{t,i}} = 0, \tag{4.4}$$

respectively.

Since $m_t = m_{t,1} (t < k)$ we can transform (4.4) into (4.3) by multiplying through by $x_{t,1}^{m_t}$; thus there are $(p^n - 1)$ distinct solutions of (4.3) for each solution of (4.4). For each solution of (4.3) we obtain a solution of (4.4) by dividing through by the same quantity, hence we have

LEMMA 4.1. *If H_t and G_t are the number of distinct non-zero solutions of* (4.3) *and* (4.4) *respectively and $m_{t,1} \equiv 0 \pmod{m_{t,i}}$ $(i = 2, \ldots, s_t)$, then*

$$H_t = (p^n - 1)G_t.$$

Let $M = m_2 \ldots m_k$, $k \geqslant 2$; since $(m_1, M) = 1$, it is known that there exist numbers a and b such that

$$am_1 + bM = 1, \qquad (a, p^n - 1) = 1. \tag{4.5}$$

Since $(a, p^n - 1) = 1$, we can determine $y_{t,i}$ in $F(p^n)$, such that

$$\begin{aligned} x_{1,1} &= y_{1,1}^{a}, \\ x_{1,i} &= y_{1,i} y_{1,1}^{am_1/m_{1,i}}, && i > 1, \\ x_{t,i} &= y_{t,i} y_{1,1}^{-bM/m_{t,i}}, && t > 1, \text{ for any } i. \end{aligned}$$

If we substitute the above relations in (4.1) and reduce by (4.5), we have

$$y_{1,1}\left(c_{1,1} + \sum_{i=2}^{s_1} c_{1,i} y_{1,i}^{m_{1,i}}\right) + \sum_{t=2}^{k} \sum_{i=1}^{s_t} c_{t,i} y_{t,i}^{m_{t,i}} = 0. \tag{4.6}$$

For the

$$(p^n - 1)^{s_2 + \ldots + s_k} - N_{2,k}$$

values of $y_{t,i}$ $(t > 1)$ for which

$$\sum_{t=2}^{k} h_t \not\equiv 0,$$

and the

$$(p^n - 1)^{s_1 - 1} - G_1$$

values of $y_{1,i}$ $(i > 1)$ for which $g_1 \not\equiv 0$, there exists a unique $y_{1,1}$. For the $N_{2,k}$ values of $y_{t,i}$ $(t > 1)$ for which

$$\sum_{t=2}^{k} h_t = 0,$$

and the G_1 values of $y_{1,i}$ $(i > 1)$ for which $g_1 = 0$, there are $p^n - 1$ values of $y_{1,1}$. Consequently we have

$$N_{1,k} = \{(p^n - 1)^{s_2 + \ldots + s_k} - N_{2,k}\}\{(p^n - 1)^{s_1 - 1} - G_1\} + (p^n - 1)N_{2,k}G_1.$$

In view of Lemma 4.1 we write

$$\begin{aligned} N_{1,k} = {} & p^{-n}(p^n - 1)^{s_2 + \ldots + s_k} \\ & + \{(p^n - 1)^{s_1} - p^n H_1\}\{(p^n - 1)^{s_2 + \ldots + s_k} - p^n N_{2,k}\}/p^n(p^n - 1). \end{aligned}$$

We obtain by induction,

THEOREM 4.1. *If $N_{1,k}$ and H_t denote the number of distinct non-zero solutions in $F(p^n)$ of* (4.1) *and* (4.3) *respectively, if m_t is the least common multiple of $m_{t,i}$ with $(m_t, m_r) = 1 (t \neq r)$, and if $m_t = m_{t,1}$ $(t < k)$, then*

$$N_{1,k} = p^{-n}(p^n - 1)^{s_1+\cdots+s_k} + \frac{(-1)^k}{p^n(p^n-1)^{k-1}} \prod_{t=1}^{k} \{(p^n - 1)^{s_t} - p^n H_t\}.$$

This recursion formula has a distinct advantage in that H_t is the number of solutions of an equation whose coefficients are in the original equation. It enables us to give the exact values of the number of solutions in a great variety of special cases; we shall give two of these here.

Let N be the number of distinct non-zero solutions in $F(p^n)$ of

$$\sum_{t=1}^{k} \sum_{i=1}^{s_t} x_{t,i}^{m_t} = 0,$$

where n is even, $p^{\frac{1}{2}n} + 1 \equiv 0 \pmod{m_t}$ $(t = 1, \ldots, k)$, and $(m_t, m_r) = 1$ $(t \neq r)$. Then we have, by (2.6),

$$H_t = (p^n - 1)\{(p^n - 1)^{s_t - 1} m_t + (p^{\frac{1}{2}n} m_t - p^{\frac{1}{2}n} - 1)^{s_t} + (m_t - 1)(-p^{\frac{1}{2}n} - 1)^{s_t}\}/m_t p^n$$

in Theorem 4.1.

In order to apply this theorem to a second special case we shall first find the number of solutions of

$$x_1^{c_1 m} - x_2^{c_2 m} = 0 \tag{4.7}$$

in $F(p^n)$, where $(c_1, c_2) = 1$ and $p^n - 1 \equiv 0 \pmod{c_i m}$ for each i. Since $(c_1, c_2) = 1$, there exist integers a and b such that $ac_1 + bc_2 = 1$, where $(a, p^n - 1) = 1$. We can determine y_1 and y_2 such that $x_1 = y_1^a$ and $x_2 = y_2 y_1^{-b}$; if we substitute these values in (4.7), we then have

$$y_1^m = y_2^{c_2 m}.$$

For the $p^n - 1$ distinct values of y_2 there are m values of y_1. Thus if H is the number of distinct non-zero solutions of (4.7), then

$$H = (p^n - 1)m. \tag{4.8}$$

If N denotes the number of distinct non-zero solutions in $F(p^n)$ of

$$\sum_{t=1}^{k} (x_{t,1}^{a_t m_t} - x_{t,2}^{m_t}) = 0,$$

with $(a_r m_r, a_t m_t) = 1$ $(r \neq t)$, then from Theorem 4.1 and (4.8) we obtain

$$N = (1/p^n)(p^n - 1)^{2k} + (-1)^k (p^n - 1)(1/p^n) \prod_{t=1}^{k} (p^n - 1 - p^n m_t).$$

This method is extremely useful in investigating trinomial equations of the type (1.1) with $c = 0$. We can give explicit formulae for the number of non-zero solutions in the case $(m_1, m_2 m_3) = 1$ and in general reduce the exponents, except in the case where one exponent is divisible by the other two.

References

1. O. B. Faircloth and H. S. Vandiver, *On the multiplicative properties of a generalized Jacobi-Cauchy cyclotomic sum*, Proc. Nat. Acad. Sci., vol. 36 (1950), 260-267.
2. L. K. Hua and H. S. Vandiver, *Characters over certain types of rings with application to the theory of equations in a finite field*, Proc. Nat. Acad. Sci., vol. 35 (1949), 94-99.
3. ———, *On the number of solutions of some trinomial equations in a finite field*, Proc. Nat. Acad. Sci., vol. 35 (1949), 477-481.
4. ———, *On the nature of the solutions of certain equations in a finite field*, Proc. Nat. Acad. Sci., vol. 35 (1949), 481-487.
5. H. H. Mitchell, *On the generalized Jacobi-Kummer cyclotomic function*, Trans. Amer. Math. Soc., vol. 17 (1916), 165-177.
6. H. S. Vandiver, *On the number of solutions of some general types of equations in a finite field*, Proc. Nat. Acad. Sci., vol. 32 (1946), 47-52.
7. ———, *On a generalization of a Jacobi exponential sum associated with cyclotomy*, Proc. Nat. Acad. Sci., vol. 36 (1950), 144-151.
8. A. Weil, *Number of solutions of equations in a finite field*, Bull. Amer. Math. Soc., vol. 55 (1949), 497-508.
9. A. L. Whiteman, *Finite Fourier series and cyclotomy*, Proc. Nat. Acad. Sci., vol. 37 (1951), 375-378.

The University of Texas

ABELIAN QUADRATIC FORMS

K. G. RAMANATHAN

1. Introduction. Hermite [4] in the course of his investigations on the transformation theory of abelian functions, introduced the notion of abelian quadratic forms. They are quadratic forms whose matrices $\mathfrak{S}$ of orders $2n$, satisfy

$$\mathfrak{S}'\mathfrak{J}\mathfrak{S} = k\mathfrak{J}, \qquad \mathfrak{J} = \begin{pmatrix} \mathfrak{O} & \mathfrak{E} \\ -\mathfrak{E} & \mathfrak{O} \end{pmatrix}$$

where $k \neq 0$ is a real number, and $\mathfrak{E}$ is the unit matrix of order n. Laguerre [7] and, more systematically, Cotty [3] developed an arithmetical theory of abelian forms in four variables. Cotty defined equivalence of abelian forms under what is now known as Siegel's modular group of degree 2 and proved the finiteness of the number of classes of integral abelian forms of given determinant. Siegel's generalization [10] of the theory of elliptic modular functions enables us to discuss completely the reduction theory of abelian forms. The object of the present note is to point out how Siegel's ideas are related to the reduction theory of abelian forms. We define equivalence of abelian forms under Siegel's modular group of degree n and obtain, for reduced abelian forms, properties analogous to those of Minkowski and Gauss. H. J. S. Smith (see [6, pp. 243-269]) showed how Gauss's theory of positive binary forms is related to the well-known modular division of the upper half of the complex z-plane. The generalization of this idea leads to Siegel's symplectic geometry. We also deal with another generalization of the theory of binary quadratic forms which is related to the hermitian modular group studied recently by H. Braun [1]. The researches of Siegel on discontinuous groups show that analogous results may be obtained by considering coset spaces of certain linear groups. In particular we consider the space of cosets of a generalized complex, orthogonal group with regard to a maximal compact subgroup and study reduction in this space in regard to a discontinuous group. We do not consider this at great length since sufficient arithmetical properties of these discontinuous groups are not known.

2. Notation. Symmetric or hermitian matrices shall be denoted by capital German letters, $\mathfrak{S}, \mathfrak{H}, \ldots$ etc. Small German letters $\mathfrak{x}, \mathfrak{y}, \ldots$ shall denote column vectors. $\mathfrak{S}[\mathfrak{C}]$ and $\mathfrak{S}\{\mathfrak{C}\}$ shall stand for $\mathfrak{C}'\mathfrak{S}\mathfrak{C}$ and $\mathfrak{C}^*\mathfrak{S}\mathfrak{C}$ where $\mathfrak{C}'$ stands for the transpose of $\mathfrak{C}$. By a triangle matrix we shall always mean a square matrix $\mathfrak{C} = (c_{kl})$ such that $c_{kl} = 0$ if $k > l$, $c_{kk} = 1$ $(k = 1, \ldots, m)$ and the rest arbitrary. $\mathfrak{W} = (w_{kl})$ shall stand for the $n \times n$ square matrix with $w_{kl} = 1$ if $k + l = n + 1$, otherwise zero. $\mathfrak{E}$ will denote the unit matrix and $\mathfrak{O}$ the zero matrix of order evident from the context. The diagonal elements of a matrix will be written with single subscripts.

Received March 26, 1951.

3. **Generalized symplectic matrices.** Let K be a field of characteristic $\neq 2$ and $G(n, K)$ the group of matrices $\mathfrak{M}$, of order $2n$, with elements in K and satisfying

$$\mathfrak{M}'\mathfrak{J}\mathfrak{M} = k\mathfrak{J}, \qquad \mathfrak{J} = \begin{pmatrix} \mathfrak{O} & \mathfrak{E} \\ -\mathfrak{E} & \mathfrak{O} \end{pmatrix}, \tag{1}$$

where $k \neq 0$ is an element of K, and $\mathfrak{E}$ is the unit matrix of order n. We shall call $G(n, K)$ the *generalized K-symplectic group* and its elements the *generalized K-symplectic matrices*. It is evident that since $\mathfrak{J}^2 = -\mathfrak{E}_{2n}$, $G(n, K)$ contains $\mathfrak{M}$ and $\mathfrak{M}'$. Consequently if

$$\mathfrak{M} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{C} & \mathfrak{D} \end{pmatrix},$$

where $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ are $n \times n$ matrices then

$$\begin{aligned} &\mathfrak{A}'\mathfrak{C} = \mathfrak{C}'\mathfrak{A}, \quad \mathfrak{D}'\mathfrak{B} = \mathfrak{B}'\mathfrak{D}, \quad \mathfrak{A}'\mathfrak{D} - \mathfrak{C}'\mathfrak{B} = k\mathfrak{E}, \\ &\mathfrak{A}\mathfrak{B}' = \mathfrak{B}\mathfrak{A}', \quad \mathfrak{C}\mathfrak{D}' = \mathfrak{D}\mathfrak{C}', \quad \mathfrak{A}\mathfrak{D}' - \mathfrak{B}\mathfrak{C}' = k\mathfrak{E}. \end{aligned} \tag{2}$$

It is evident that if $n = 1$ the relation (1) is satisfied automatically provided k is the determinant of $\mathfrak{M}$. In the general case we shall call k the *kernel* of the generalized symplectic matrix $\mathfrak{M}$. Let us call $\mathfrak{M}$ a *K-symplectic matrix* if $\mathfrak{M}$ has kernel unity. The K-symplectic matrices form a subgroup of $G(n, K)$. Let us call a generalized K-symplectic matrix $\mathfrak{S}$ *abelian* if it is symmetric. Then for $\mathfrak{S}$ abelian we have

$$\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}, \quad \mathfrak{A}\mathfrak{B}' = \mathfrak{B}\mathfrak{A}, \quad \mathfrak{A}\mathfrak{C} - \mathfrak{B}^2 = k\mathfrak{E}. \tag{3}$$

k is called the kernel of the abelian form $\mathfrak{x}'\mathfrak{S}\mathfrak{x}$. We shall show that every abelian matrix can, by a K-symplectic transformation, be reduced to the diagonal form. In case $n = 1$ this result is trivial since any two-rowed, square matrix of determinant unity is symplectic.

THEOREM 1. *If $\mathfrak{S}$ is a K-abelian matrix, there exists a K-symplectic matrix $\mathfrak{P}$ with*

$$\mathfrak{P}'\mathfrak{S}\mathfrak{P} = \begin{pmatrix} \mathfrak{D} & \mathfrak{O} \\ \mathfrak{O} & k\mathfrak{D}^{-1} \end{pmatrix}, \tag{4}$$

where $\mathfrak{D}$ is a diagonal matrix with elements in K and k is the kernel of $\mathfrak{S}$.

Proof. Let $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$, $\mathfrak{A} = \begin{pmatrix} a & \mathfrak{a}' \\ \mathfrak{a} & \mathfrak{A}_1 \end{pmatrix}$, and $\mathfrak{B} = \begin{pmatrix} b & \mathfrak{b}' \\ \mathfrak{y} & \mathfrak{B}_1 \end{pmatrix}$, $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{y}$ being column vectors of $n-1$ rows. Let us assume $a \neq 0$. Then $\mathfrak{A} = \begin{pmatrix} a & 0 \\ 0 & \mathfrak{A}_2 \end{pmatrix}\begin{pmatrix} 1 & -a^{-1}\mathfrak{a}' \\ 0 & \mathfrak{E}_{n-1} \end{pmatrix}$ where $\mathfrak{A}_2 = \mathfrak{A}_1 - a^{-1}\mathfrak{a}\mathfrak{a}'$. Let $\mathfrak{B} = \begin{pmatrix} 1 & -a^{-1}\mathfrak{a}' \\ 0 & \mathfrak{E} \end{pmatrix}$ then $\mathfrak{Q}_1 = \begin{pmatrix} \mathfrak{B} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{B}'^{-1} \end{pmatrix}$ is K-symplectic. Let

$$\mathfrak{Q}_1'\mathfrak{S}\mathfrak{Q}_1 = \begin{pmatrix} \mathfrak{A}_0 & \mathfrak{B}_0 \\ \mathfrak{B}_0' & \mathfrak{C}_0 \end{pmatrix}. \tag{5}$$

Then $\mathfrak{A}_0 = \begin{pmatrix} a & 0 \\ 0 & \mathfrak{A}_2 \end{pmatrix}$ and $\mathfrak{B}_0 = \begin{pmatrix} b & b' \\ a^{-1}\mathfrak{A}_2 b & \mathfrak{B}_1 - a^{-1}ab' \end{pmatrix}$. Let $\mathfrak{T}$ be the symmetric matrix $\mathfrak{T} = a^{-1}\begin{pmatrix} -b & -b' \\ -b & 0 \end{pmatrix}$ and let $\mathfrak{Q}_2 = \begin{pmatrix} \mathfrak{E}_n & \mathfrak{T} \\ 0 & \mathfrak{E} \end{pmatrix}$ be a K-symplectic matrix. Then

$$\mathfrak{Q}_2'\mathfrak{Q}_1'\mathfrak{S}\mathfrak{Q}_1\mathfrak{Q}_2 = \begin{pmatrix} \mathfrak{A}_0 & \mathfrak{B}_2 \\ \mathfrak{B}_2' & \mathfrak{C}_2 \end{pmatrix}, \tag{6}$$

where $\mathfrak{B}_2 = \begin{pmatrix} 0 & 0 \\ 0 & a^{-1}ab' - \mathfrak{B}_1 \end{pmatrix}$ and $\mathfrak{C}_2 = \begin{pmatrix} a^{-1}k & 0 \\ 0 & \mathfrak{C}_2 \end{pmatrix}$. Thus $\begin{pmatrix} \mathfrak{A}_0 & \mathfrak{B}_2 \\ \mathfrak{B}_2' & \mathfrak{C}_2 \end{pmatrix}$ is an abelian matrix of kernel k and is an element of $G(n-1, K)$. Also $\mathfrak{B}_2 = a^{-1}ab' - \mathfrak{B}_1$. It is now evident how the proof can be completed by induction provided we can show that by a K-symplectic transformation we can make the first diagonal element of $\mathfrak{A}$ not zero.

Suppose that the first diagonal element of $\mathfrak{A}$ is zero but not its pth diagonal element $1 < p \leqslant n$. Let $\mathfrak{U}$ be the matrix interchanging the first and the pth columns of $\mathfrak{A}$. Then $\mathfrak{S}\begin{bmatrix} \mathfrak{U} & 0 \\ 0 & \mathfrak{U}'^{-1} \end{bmatrix}$ has its first diagonal element not zero. Suppose now that all the diagonal elements of $\mathfrak{A}$ were zero. Let an element in the kth row and lth column of $\mathfrak{A}$ be not zero. By a transformation interchanging the first and lth column we may assume that an element in the first row and lth column is not zero. Put $\mathfrak{U} = \begin{pmatrix} 1 & 0 \\ \mathfrak{y}_1 & \mathfrak{E} \end{pmatrix}$ where $\mathfrak{y}_1$ is a column vector of $n-1$ rows with zero everywhere except in the $(l-1)$th row. Then $\mathfrak{S}\begin{bmatrix} \mathfrak{U} & 0 \\ 0 & \mathfrak{U}'^{-1} \end{bmatrix}$ has its first diagonal element not zero provided the characteristic of K is not two.

We therefore come to the case $\mathfrak{A} = 0$. Then $\mathfrak{J}'\mathfrak{S}\mathfrak{J} = \begin{pmatrix} \mathfrak{C} & -\mathfrak{B}' \\ -\mathfrak{B} & \mathfrak{A} \end{pmatrix}$ and we can apply the arguments in the last paragraph to $\mathfrak{C}$. Let now $\mathfrak{A} = 0 = \mathfrak{C}$. Then $|\mathfrak{B}| \neq 0$. Let $\mathfrak{P}_1 = \begin{pmatrix} \mathfrak{E} & 0 \\ \mathfrak{F} & \mathfrak{E} \end{pmatrix}$ be K-symplectic then $\mathfrak{F}$ is symmetric. $\mathfrak{S}[\mathfrak{P}_1] = \begin{pmatrix} \mathfrak{B}\mathfrak{F} + \mathfrak{F}\mathfrak{B}' & * \\ * & * \end{pmatrix}$. Let $\mathfrak{x}$ be the column vector

$$\mathfrak{x} = \mathfrak{B}^{-1}\begin{pmatrix} 1 \\ 0 \\ \cdots \\ 0 \end{pmatrix}$$

and let $\mathfrak{F}$ have $\mathfrak{x}$ for first row and column and zeros elsewhere. Then the first diagonal element of $\mathfrak{S}[\mathfrak{P}_1]$ is not zero since K has characteristic $\neq 2$.

Our theorem is thus completely established.

The theorem could have been proved much more simply if K had not been a finite field, but since this result would be of use in the analytic theory of abelian forms we have given a proof valid even for finite fields.

COROLLARY. *If K is real algebraically closed*[1] *then by a generalized K-symplectic matrix $\mathfrak{Q}$ we can make $\mathfrak{S}[\mathfrak{Q}]$ have the diagonal form with ± 1 in the diagonals.*

Theorem 1 tells us that the determinant of a K-abelian matrix is

$$|\mathfrak{S}| = |\mathfrak{AC} - \mathfrak{B}^2| = k^n. \tag{7}$$

Let now $K_0 = K(\sqrt{d})$ where d is an element of K and $\sqrt{d}$ is not in K. Let σ be the generating automorphism of K_0/K so that $\sigma^2 = 1$, the identity automorphism. Let $\mathfrak{M}^{(2n)} = \mathfrak{M}$ be a matrix with elements in K_0 and denote $\mathfrak{M}^*$ by

$$\mathfrak{M}^* = (m_{ik}^{\sigma}) \tag{8}$$

where $\mathfrak{M} = (m_{ik})$. Then $\mathfrak{M}^{**} = \mathfrak{M}$, $(\mathfrak{M}_1\mathfrak{M}_2)^* = \mathfrak{M}_2^*\mathfrak{M}_1^*$, and $(\mathfrak{M}^*)^{-1} = (\mathfrak{M}^{-1})^*$. Let $G(n, K_0)$ be the set of matrices $\mathfrak{M}$ of order $2n$ such that

$$\mathfrak{M}^*\mathfrak{J}\mathfrak{M} = k\mathfrak{J} \tag{9}$$

where $k \neq 0$ is in K. The number k is called the *kernel* of $\mathfrak{M}$. The matrices $\mathfrak{M}$ of kernel unity are called *K_0-hermitian symplectic*. If $\mathfrak{S}$ is a matrix in $G(n, K_0)$ such that $\mathfrak{S}^* = \mathfrak{S}$ we shall call $\mathfrak{S}$ *a K_0-abelian hermitian matrix*. The analogue of Theorem 1 then is

THEOREM 1′. *Any abelian hermitian matrix $\mathfrak{S}$ can by a K_0-hermitian symplectic transformation $\mathfrak{Q}$ be brought into the diagonal form; that is,*

$$\mathfrak{Q}^*\mathfrak{S}\mathfrak{Q} = \begin{pmatrix} \mathfrak{D} & \mathfrak{O} \\ \mathfrak{O} & k\mathfrak{D}^{-1} \end{pmatrix} \tag{10}$$

where $\mathfrak{D}$ is a diagonal matrix with elements in K.

The proof of this theorem is similar to that of Theorem 1. For an abelian hermitian matrix $\mathfrak{S}$ we have

$$\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}^* & \mathfrak{C} \end{pmatrix}, \quad |\mathfrak{S}| = |\mathfrak{AC} - \mathfrak{B}^2| = k^n. \tag{11}$$

4. Matrices over the real field. Let us now assume that K is the field of all real numbers. Let $G(n, K)$ denote the group of real matrices $\mathfrak{M}$ satisfying (1). The real number k is the kernel of $\mathfrak{M}$. $\mathfrak{M}$ is called a real *generalized symplectic matrix*. The subgroup of $G(n, K)$ with kernel unity is the well-known real symplectic group. We shall prove

LEMMA 1. *The determinant $|\mathfrak{M}|$ of a general symplectic matrix $\mathfrak{M}$ of kernel k is k^n.*

Proof. Let $\mathfrak{M} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{C} & \mathfrak{D} \end{pmatrix}$ have kernel k. Let $\mathfrak{P} = \begin{pmatrix} \mathfrak{E} & \mathfrak{O} \\ t\mathfrak{E} & \mathfrak{E} \end{pmatrix}$, with t a real number different from zero, be a symplectic matrix. Then $|\mathfrak{P}| = 1$; also $\mathfrak{M}\mathfrak{P} = \begin{pmatrix} \mathfrak{A}+t\mathfrak{B} & * \\ * & * \end{pmatrix}$.

[1] We use the term real algebraically closed in the sense of Artin and Schreier. See [12, p. 235].

Since $|\mathfrak{A} + t\mathfrak{B}| = 0$ has only finitely many real solutions t, it follows that there is a real $t \neq 0$ with $|\mathfrak{A} + t\mathfrak{B}| \neq 0$. Let t be such a real number. Put $\mathfrak{M}\mathfrak{P} = \begin{pmatrix} \mathfrak{A}_1 & \mathfrak{B}_1 \\ \mathfrak{C}_1 & \mathfrak{D}_1 \end{pmatrix}$, $|\mathfrak{A}_1| \neq 0$ and consider $\mathfrak{Q} = \begin{pmatrix} \mathfrak{E} & -\mathfrak{A}_1^{-1}\mathfrak{B}_1 \\ \mathfrak{O} & \mathfrak{E} \end{pmatrix}$. Since $\mathfrak{M}\mathfrak{P}$ is generalized symplectic, $\mathfrak{A}_1\mathfrak{B}'_1 = \mathfrak{B}_1\mathfrak{A}'_1$ or $\mathfrak{A}_1^{-1}\mathfrak{B}_1$ is symmetric. Consequently, $\mathfrak{Q}$ is a real symplectic matrix. Now

$$\mathfrak{M}\mathfrak{P}\mathfrak{Q} = \begin{pmatrix} \mathfrak{A}_1 & \mathfrak{O} \\ \mathfrak{C}_1 & \mathfrak{D}_1 - \mathfrak{C}_1\mathfrak{A}_1^{-1}\mathfrak{B}_1 \end{pmatrix}. \tag{12}$$

But from (2) it follows that $\mathfrak{D}_1 - \mathfrak{C}_1\mathfrak{A}_1^{-1}\mathfrak{B}_1 = k\mathfrak{A}'_1{}^{-1}$. Since $|\mathfrak{Q}| = 1$ our contention in the lemma follows.

COROLLARY. *If $\mathfrak{M}$ is symplectic then* $|\mathfrak{M}| = 1$.

Let us call *modular* any real symplectic matrix whose elements are rational integers. The modular matrices obviously form a group called the *modular group of degree n*. For any modular matrix $\mathfrak{M}$, we have $|\mathfrak{M}| = 1$.

Call two $n \times n$ matrices $\mathfrak{C}$ and $\mathfrak{D}$ with rational elements a *symmetric pair* if $(\mathfrak{C}\ \mathfrak{D})$ is of rank n and

$$\mathfrak{C}\mathfrak{D}' = \mathfrak{D}\mathfrak{C}'. \tag{13}$$

If $\mathfrak{C}, \mathfrak{D}$ is an integral symmetric pair, there exists a non-singular integral matrix $\mathfrak{P}$ with $\mathfrak{P}^{-1}(\mathfrak{C}\ \mathfrak{D})$ a primitive matrix. We call $\mathfrak{P}$ the *greatest common divisor* (g.c.d.) of $\mathfrak{C}$ and $\mathfrak{D}$. If $\mathfrak{P}$ is unimodular we call $\mathfrak{C}$ and $\mathfrak{D}$ coprime. The g.c.d. is unique up to multiplication on the right by a unimodular matrix. For let $\mathfrak{P}_1$ and $\mathfrak{P}_2$ be two g.c.d.'s. Then $\mathfrak{P}_1^{-1}(\mathfrak{C}\ \mathfrak{D})$ is a primitive matrix and can be completed into a unimodular matrix $\mathfrak{U}$. Put $\mathfrak{U}^{-1} = \begin{pmatrix} \mathfrak{X} & * \\ \mathfrak{Y} & * \end{pmatrix}$, then $\mathfrak{P}_1^{-1}(\mathfrak{C}\mathfrak{X} + \mathfrak{D}\mathfrak{Y}) = \mathfrak{E}$. Hence $\mathfrak{P}_2^{-1}(\mathfrak{C}\mathfrak{X} + \mathfrak{D}\mathfrak{Y}) = \mathfrak{P}_2^{-1}\mathfrak{P}_1$ is integral and similarly $\mathfrak{P}_1^{-1}\mathfrak{P}_2$. Hence our contention. We prove

LEMMA 2. *If $\mathfrak{C}, \mathfrak{D}$ is an integral symmetric pair, there is a generalized integral symplectic matrix* $\mathfrak{M} = \begin{pmatrix} * & * \\ \mathfrak{C} & \mathfrak{D} \end{pmatrix}$.

Proof. Let $\mathfrak{P}$ be the g.c.d. of $\mathfrak{C}$ and $\mathfrak{D}$. Then $\mathfrak{P}^{-1}(\mathfrak{C}\ \mathfrak{D}) = (\mathfrak{C}_1\mathfrak{D}_1)$ is a primitive matrix. Let $(\mathfrak{C}_1\mathfrak{D}_1)$ be completed into a unimodular matrix $\mathfrak{U}$ and let $\mathfrak{U}^{-1} = \begin{pmatrix} \mathfrak{X} & * \\ \mathfrak{Y} & * \end{pmatrix}$. Put

$$\mathfrak{X}_1 = \mathfrak{Y}' + \mathfrak{X}'\mathfrak{Y}\mathfrak{C}_1, \quad \mathfrak{Y}_1 = -\mathfrak{X}' + \mathfrak{X}'\mathfrak{Y}\mathfrak{D}_1.$$

Then $\begin{pmatrix} \mathfrak{X}_1 & \mathfrak{Y}_1 \\ \mathfrak{C}_1 & \mathfrak{D}_1 \end{pmatrix}$ is a modular matrix. Let t be an integer so that $t\mathfrak{P}^{-1}$ is an integral matrix. The matrix

$$\mathfrak{M} = \begin{pmatrix} t\mathfrak{P}'^{-1}\mathfrak{X}_1 & t\mathfrak{P}'^{-1}\mathfrak{Y}_1 \\ \mathfrak{C} & \mathfrak{D} \end{pmatrix}$$

satisfies our requirements and is of kernel t.

Let us now call two general integral symplectic matrices $\mathfrak{M}_1$ and $\mathfrak{M}_2$ *associated* if

$$\mathfrak{M}_1 = \mathfrak{M}_2\mathfrak{P} \tag{14}$$

with a modular $\mathfrak{P}$. We write $\mathfrak{M}_1 \sim \mathfrak{M}_2$. This is an equivalence relation since the modular matrices form a group. All integral matrices equivalent to $\mathfrak{M}_1$ form a class. Thus all generalized integral symplectic matrices fall into classes of associate matrices. The matrices in any class have the same kernel.

THEOREM 2. *The number of classes of associate matrices with a given kernel is finite.*

Proof. Let $\mathfrak{M} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{C} & \mathfrak{D} \end{pmatrix}$ have kernel k. Let $\mathfrak{P}$ be the g.c.d. of $\mathfrak{C}$ and $\mathfrak{D}$. Then $k\mathfrak{P}^{-1}$ is an integral matrix. Let $\mathfrak{X}_1, \mathfrak{X}_2$ be so chosen that $\mathfrak{C}\mathfrak{X}_1 + \mathfrak{D}\mathfrak{X}_2 = \mathfrak{P}$ and $\begin{pmatrix} \mathfrak{X}_1 \\ \mathfrak{X}_2 \end{pmatrix}$ can be completed to a modular matrix $\begin{pmatrix} \mathfrak{X}_1 & \mathfrak{X}_3 \\ \mathfrak{X}_2 & \mathfrak{X}_4 \end{pmatrix} = \mathfrak{Q}$. Then

$$\mathfrak{M}\mathfrak{Q} = \begin{pmatrix} \mathfrak{A}_1 & \mathfrak{B}_1 \\ \mathfrak{P} & \mathfrak{D}_1 \end{pmatrix}. \tag{15}$$

From (2) we get $\mathfrak{P}\mathfrak{D}'_1 = \mathfrak{D}_1\mathfrak{P}'$ and so $\mathfrak{P}^{-1}\mathfrak{D}_1 = \mathfrak{T}$ is an integral symmetric matrix. Now

$$\mathfrak{M}\mathfrak{Q}\begin{pmatrix} \mathfrak{T} & \mathfrak{E} \\ -\mathfrak{E} & \mathfrak{O} \end{pmatrix} = \begin{pmatrix} \mathfrak{A}_1\mathfrak{T} - \mathfrak{B}_1 & \mathfrak{A}_1 \\ \mathfrak{O} & \mathfrak{P} \end{pmatrix}, \tag{16}$$

and $\mathfrak{A}_1\mathfrak{T} - \mathfrak{B}_1 = k\mathfrak{P}'^{-1}$ is an integral matrix. That $\mathfrak{P}$ depends only on the class of $\mathfrak{M}$ is easy to see, for, if $\mathfrak{M}$ can be reduced to $\begin{pmatrix} \mathfrak{A}_2 & \mathfrak{B}_2 \\ \mathfrak{O} & \mathfrak{P}_2 \end{pmatrix}$ and $\begin{pmatrix} \mathfrak{A}_3 & \mathfrak{B}_3 \\ \mathfrak{O} & \mathfrak{P}_3 \end{pmatrix}$ by multiplication on the right by modular matrices, then for a suitable modular matrix $\begin{pmatrix} \mathfrak{C}_1 & \mathfrak{C}_2 \\ \mathfrak{C}_3 & \mathfrak{C}_4 \end{pmatrix}$ we have

$$\begin{pmatrix} \mathfrak{A}_2 & \mathfrak{B}_2 \\ \mathfrak{O} & \mathfrak{P}_2 \end{pmatrix}\begin{pmatrix} \mathfrak{C}_1 & \mathfrak{C}_2 \\ \mathfrak{C}_3 & \mathfrak{C}_4 \end{pmatrix} = \begin{pmatrix} \mathfrak{A}_3 & \mathfrak{B}_3 \\ \mathfrak{O} & \mathfrak{P}_3 \end{pmatrix}, \tag{17}$$

which means $\mathfrak{C}_3 = \mathfrak{O}$, $\mathfrak{C}_4$ is unimodular and $\mathfrak{P}_2\mathfrak{C}_4 = \mathfrak{P}_3$.

Let $\mathfrak{U}$ be a unimodular matrix so that $\mathfrak{P}\mathfrak{U} = \mathfrak{F} = (f_{kl})$ where $f_{kl} = 0$, $k > l$, and $0 \leqslant f_{kl} < f_k$ $(k < l = 1, \ldots, n)$. Thus

$$\mathfrak{M}\mathfrak{Q}\begin{pmatrix} \mathfrak{T} & \mathfrak{E} \\ -\mathfrak{E} & \mathfrak{O} \end{pmatrix}\begin{pmatrix} \mathfrak{U}'^{-1} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{U} \end{pmatrix} = \begin{pmatrix} k\mathfrak{F}'^{-1} & \mathfrak{H} \\ \mathfrak{O} & \mathfrak{F} \end{pmatrix} = \begin{pmatrix} \mathfrak{F}_1 & \mathfrak{H} \\ \mathfrak{O} & \mathfrak{F} \end{pmatrix}. \tag{18}$$

Now $\mathfrak{F}_1^{-1}\mathfrak{H}$ is symmetric. Consider $\begin{pmatrix} \mathfrak{E} & \mathfrak{L} \\ \mathfrak{O} & \mathfrak{E} \end{pmatrix}$ where $\mathfrak{L}$ is integral symmetric. Choose $\mathfrak{L}$ so that the elements of $\mathfrak{F}_1^{-1}\mathfrak{H} + \mathfrak{L}$ lie between $\frac{1}{2}$ and $-\frac{1}{2}$. The matrix $\begin{pmatrix} \mathfrak{F}_1 & \mathfrak{H} \\ \mathfrak{O} & \mathfrak{F} \end{pmatrix} \times \begin{pmatrix} \mathfrak{E} & \mathfrak{L} \\ \mathfrak{O} & \mathfrak{E} \end{pmatrix}$ has now only a finite number of possibilities for a given k. Our lemma is thus proved.

In the case $n = 1$ the number of these classes is $\sigma(k)$, the sum of the divisors of k. In the general case an expression for this number of classes seems to be difficult to find. Hermite and Cotty have shown that if $k = p$, a prime number, and $n = 2$, the number of classes is $1 + p + p^2 + p^3$.

5. Abelian quadratic forms. Let $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$ be a symmetric real matrix satisfying (1). It is called a real abelian matrix and the associated quadratic form, a real abelian quadratic form. Abelian forms are a generalization of binary quadratic forms. From Theorem 1 and Corollary it follows that there exists a general symplectic matrix $\mathfrak{P}$ with

$$\mathfrak{P}'\mathfrak{S}\mathfrak{P} = \begin{pmatrix} \mathfrak{D} & \mathfrak{O} \\ \mathfrak{O} & \xi\mathfrak{D} \end{pmatrix}, \tag{19}$$

where $\mathfrak{D}$ is a diagonal matrix with ± 1 in the diagonal and $\xi = \operatorname{sgn} k$. This shows that the number of negative signs in the normal form of $\mathfrak{S}$ is either $2p$ $(0 \leqslant p \leqslant n)$ or n. We can thus speak of signature of an abelian matrix without any fear of confusion.

Let $\mathfrak{S}$ be an abelian matrix and $\mathfrak{x}'\mathfrak{S}\mathfrak{x}$ the abelian quadratic form. We say that $\mathfrak{x}'\mathfrak{S}\mathfrak{x}$ is *positive* (*negative*) *definite* if $\mathfrak{x}'\mathfrak{S}\mathfrak{x} > 0 (< 0)$ for real $\mathfrak{x} \neq 0$. It is obvious that a necessary and sufficient condition for positivity is that $k > 0$ and $\mathfrak{A}$ is positive definite. Consequently $|\mathfrak{A}| \neq 0$. Abelian matrices that are not definite are *indefinite*.

Let $\mathfrak{P}$ be a modular matrix. With $\mathfrak{S}$, $\mathfrak{S}[\mathfrak{P}]$ is also abelian. We call two abelian matrices $\mathfrak{S}_1$ and $\mathfrak{S}_2$ *symplectic equivalent*[2] if there is a modular matrix $\mathfrak{P}$ with $\mathfrak{S}_1[\mathfrak{P}] = \mathfrak{S}_2$. This is an equivalence relation and all abelian matrices can be put into classes of equivalent matrices. Let us first confine ourselves to positive abelian forms. It will be observed that our method is a simple generalization of Gauss's theory.

If $ax^2 + 2bxy + cy^2$ is a positive binary form, Gauss's method of reduction consists in first finding an equivalent form with a minimum and then transforming it so that $b/a \leqslant \frac{1}{2}$. We adopt the same procedure.

Let $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$ be positive abelian with arbitrary real elements and let $\mathfrak{P}'$, $\mathfrak{Q}'$ be an integral symmetric pair. Put $\mathfrak{L} = \begin{pmatrix} \mathfrak{P} \\ \mathfrak{Q} \end{pmatrix}$. Consider the determinant of

$$\mathfrak{S}[\mathfrak{L}] = \mathfrak{P}'\mathfrak{A}\mathfrak{P} + \mathfrak{Q}'\mathfrak{B}'\mathfrak{P} + \mathfrak{P}'\mathfrak{B}\mathfrak{Q} + \mathfrak{Q}'\mathfrak{C}\mathfrak{Q}. \tag{20}$$

If for a $\mathfrak{P}$, $\mathfrak{Q}$ this determinant is a minimum at all, then this minimum will be attained when $\mathfrak{L}$ is primitive or $\mathfrak{P}'$, $\mathfrak{Q}'$ is a coprime pair. For if $\mathfrak{R}'$ is the g.c.d. of $\mathfrak{P}'$, $\mathfrak{Q}'$ then $\mathfrak{L}\mathfrak{R}^{-1} = \begin{pmatrix} \mathfrak{P} \\ \mathfrak{Q} \end{pmatrix}\mathfrak{R}^{-1}$ and

[2]Using the terminology of Gauss we may call this *proper equivalence*. Hermite and Cotty actually consider equivalence under integral matrices $\mathfrak{P}$ satisfying $\mathfrak{P}'\mathfrak{J}\mathfrak{P} = \pm\mathfrak{J}$. But since the modular matrices form a subgroup of index 2 in this group of $\mathfrak{P}$, there is not much change in our argument if we consider $\mathfrak{P}$ with negative kernel.

$$|\mathfrak{S}[\mathfrak{L}\mathfrak{R}^{-1}]| < |\mathfrak{S}[\mathfrak{L}]|. \tag{21}$$

So for investigating the minimum of $|\mathfrak{S}[\mathfrak{L}]|$ it will be enough if we confine ourselves to the case when $\mathfrak{P}'$, $\mathfrak{Q}'$ are coprime.

If $|\mathfrak{S}[\mathfrak{L}]|$ is minimum then this minimum will not be altered if we change $\mathfrak{L}$ into $\mathfrak{L}\mathfrak{U}$ with $\mathfrak{U}$ unimodular. Then $\mathfrak{S}[\mathfrak{L}] = \mathfrak{A}_1$ is changed into $\mathfrak{U}'\mathfrak{A}_1\mathfrak{U}$. Since $\mathfrak{A}_1$ is positive definite we can by a proper choice of $\mathfrak{U}$ make $\mathfrak{U}'\mathfrak{A}_1\mathfrak{U}$ reduced in the sense of Minkowski. The coprimality of $\mathfrak{P}'$, $\mathfrak{Q}'$ is unaltered by this. We shall now prove

LEMMA 3. *If* $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$ *is positive abelian then there exists an* $\mathfrak{L} = \begin{pmatrix} \mathfrak{P} \\ \mathfrak{Q} \end{pmatrix}$ *with* $\mathfrak{P}'$, $\mathfrak{Q}'$ *coprime such that* $|\mathfrak{L}'\mathfrak{S}\,\mathfrak{L}|$ *is minimum.*

Proof. Let $\mathfrak{L}'\mathfrak{S}\,\mathfrak{L} = \mathfrak{A}_1$. In order to prove the lemma we may assume that $\mathfrak{A}_1$ is reduced in the sense of Minkowski. Let $a > 0$ be a large real number. We shall show that $|\mathfrak{A}_1| < a$ has only a finite number of integral solutions $\mathfrak{L}$.

Now

$$\mathfrak{A}_1 = \mathfrak{L}'\mathfrak{S}\mathfrak{L} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}\begin{bmatrix} \mathfrak{P} \\ \mathfrak{Q} \end{bmatrix} = \begin{pmatrix} \mathfrak{A} & \mathfrak{O} \\ \mathfrak{O} & k\mathfrak{A}^{-1} \end{pmatrix}\begin{bmatrix} \mathfrak{P} + \mathfrak{A}^{-1}\mathfrak{B}\mathfrak{Q} \\ \mathfrak{Q} \end{bmatrix}, \tag{22}$$

so that

$$\mathfrak{A}_1 = \mathfrak{A}[\mathfrak{P} + \mathfrak{A}^{-1}\mathfrak{B}\mathfrak{Q}] + k\mathfrak{A}^{-1}[\mathfrak{Q}]. \tag{23}$$

Let $\mathfrak{A}_1 = (a_{kl})$ and write $\mathfrak{p}_l$ and $\mathfrak{q}_l$ for the lth columns of $\mathfrak{P}$ and $\mathfrak{Q}$ respectively. Then from (23) we get

$$a_l = \mathfrak{A}[\mathfrak{p}_l + \mathfrak{A}^{-1}\mathfrak{B}\mathfrak{q}_l] + k\mathfrak{A}^{-1}[\mathfrak{q}_l]. \tag{24}$$

Since $\mathfrak{A}_1$ is reduced in the sense of Minkowski we get

$$a_1 a_2 \ldots a_n \leqslant \lambda_n |\mathfrak{A}_1| < \lambda_n a = b, \tag{25}$$

λ_n being a constant depending only on n. Since $\mathfrak{A}^{-1}$ is a positive real matrix there exists a $d > 0$ such that for any integral column $\mathfrak{q}$, $d \leqslant k\mathfrak{A}^{-1}[\mathfrak{q}]$. Thus from (24) we get

$$d \leqslant a_1 \leqslant a_2 \leqslant \ldots \leqslant a_n. \tag{26}$$

Since the right side of (24) consists of two positive numbers,

$$\begin{cases} \mathfrak{A}[\mathfrak{p}_l + \mathfrak{A}^{-1}\mathfrak{B}\mathfrak{q}_l] \leqslant a_l, \\ k\mathfrak{A}^{-1}[\mathfrak{q}_l] \leqslant a_l. \end{cases} \tag{27}$$

Using (25), (26), and (27) it follows that

$$a_l \leqslant (b/d^{l-1})^{1/(n-l+1)} = b_l, \tag{28}$$

where b_l depends only on n, $\mathfrak{A}$, and a. From (27) and (28) our assertion follows.

We shall now outline a reduction theory of positive abelian forms. Let $\mathfrak{S} = \begin{pmatrix} \mathfrak{A}_0 & \mathfrak{B}_0 \\ \mathfrak{B}'_0 & \mathfrak{C}_0 \end{pmatrix}$ be a positive abelian matrix and let $\mathfrak{M} = \begin{pmatrix} \mathfrak{P}_1 & \mathfrak{P}_3 \\ \mathfrak{P}_2 & \mathfrak{P}_4 \end{pmatrix}$ run through all modular matrices. Consider the first "columns" $\begin{pmatrix} \mathfrak{P}_1 \\ \mathfrak{P}_2 \end{pmatrix}$ of these modular matrices. Let $\mathfrak{S}\begin{bmatrix} \mathfrak{P}_1 \\ \mathfrak{P}_2 \end{bmatrix}$ have a minimum determinant. By Lemma 3 there are only a finite number of such first columns. Transform, if necessary, by a matrix $\begin{pmatrix} \mathfrak{U} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{U}'^{-1} \end{pmatrix}$, where $\mathfrak{U}$ is a unimodular matrix, so that $\mathfrak{S}\begin{bmatrix} \mathfrak{P}_1\mathfrak{U} \\ \mathfrak{P}_2\mathfrak{U} \end{bmatrix}$ is reduced in the sense of Minkowski. Write

$$\mathfrak{S}\left[\mathfrak{M}\begin{pmatrix} \mathfrak{U} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{U}'^{-1} \end{pmatrix}\right] = \begin{pmatrix} \mathfrak{A}_1 & \mathfrak{B}_1 \\ \mathfrak{B}'_1 & \mathfrak{C}_1 \end{pmatrix} = \mathfrak{S}_1, \tag{29}$$

so that $|\mathfrak{A}_1|$ is minimum and $\mathfrak{A}_1$ is reduced in the sense of Minkowski. All modular matrices whose first columns $\begin{pmatrix} \mathfrak{P} \\ \mathfrak{Q} \end{pmatrix}$ are the same as that of $\mathfrak{M}\begin{pmatrix} \mathfrak{U} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{U}'^{-1} \end{pmatrix}$ are of the form

$$\mathfrak{M}\begin{pmatrix} \mathfrak{U} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{U}'^{-1} \end{pmatrix}\begin{pmatrix} \mathfrak{E} & \mathfrak{T} \\ \mathfrak{O} & \mathfrak{E} \end{pmatrix} = \mathfrak{M}_1, \tag{30}$$

where $\mathfrak{T}$ is an integral symmetric matrix. Let $\mathfrak{S}_1\begin{bmatrix} \mathfrak{E} & \mathfrak{T} \\ \mathfrak{O} & \mathfrak{E} \end{bmatrix} = \begin{pmatrix} \mathfrak{A}_1 & \mathfrak{B}_2 \\ * & * \end{pmatrix}$; then

$$\mathfrak{B}_2 = \mathfrak{A}_1\mathfrak{T} + \mathfrak{B}_1, \tag{31}$$

so that $\mathfrak{A}_1^{-1}\mathfrak{B}_1$ and $\mathfrak{A}_1^{-1}\mathfrak{B}_2$ are two symmetric matrices which are congruent modulo 1. Thus the integral matrix $\mathfrak{T}$ can be chosen in such a way that the elements of $\mathfrak{A}_1^{-1}\mathfrak{B}_2$ lie between $+\frac{1}{2}$ and $-\frac{1}{2}$. If $\mathfrak{A}_1$ and $\mathfrak{B}_2$ are fixed, automatically the other elements of the matrix $\mathfrak{S}[\mathfrak{M}_1]$ are fixed too. We call $\mathfrak{S}[\mathfrak{M}_1] = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$, which is equivalent to $\mathfrak{S}$, a *symplectic reduced* matrix. It has the properties:

(32) (i) $|\mathfrak{A}|$ is minimum,
(ii) $\mathfrak{A}$ is reduced in the sense of Minkowski,
(iii) the elements of $\mathfrak{B}^{-1}\mathfrak{A}$ are in absolute value $\leqslant \frac{1}{2}$.

Condition (i) merely asserts that for any coprime pair, *a fortiori* for any integral symmetric pair $\mathfrak{P}$, $\mathfrak{Q}$, we have

$$\left|\begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}\begin{bmatrix} \mathfrak{P} \\ \mathfrak{Q} \end{bmatrix}\right| > |\mathfrak{A}|. \tag{33}$$

Putting $\mathfrak{P} = \mathfrak{O}$, $\mathfrak{Q} = \mathfrak{E}$ we get

$$|\mathfrak{A}| \leqslant |\mathfrak{C}|. \tag{34}$$

In order now to obtain the analogue of the fundamental Gauss-Minkowski inequality regarding the product of the diagonal elements of a reduced matrix we proceed thus.

Let $\mathfrak{P} = \begin{pmatrix} \mathfrak{E}_{n-1} & 0 \\ 0 & 0 \end{pmatrix}$, $\mathfrak{Q} = \begin{pmatrix} \mathfrak{O} & 0 \\ 0 & 1 \end{pmatrix}$. Then $\mathfrak{P}$, $\mathfrak{Q}$ are coprime. Let t be the last

diagonal element of $\mathfrak{A}^{-1}\mathfrak{B}$ and let $\mathfrak{A} = \begin{pmatrix} \mathfrak{A}_0 & a' \\ a & a \end{pmatrix}$, where $\mathfrak{A}_0$ is a symmetric matrix of $n-1$ rows. Making use of the identity (23) and the inequality (33) we get

$$|\mathfrak{A}| \leqslant k|\mathfrak{A}_0|^2/|\mathfrak{A}| + t^2|\mathfrak{A}| \tag{35}$$

Since $|t| < \frac{1}{2}$ it follows that

$$\sqrt{k}|\mathfrak{A}_0| > \tfrac{1}{2}\sqrt{3}|\mathfrak{A}|. \tag{36}$$

Let us now prove the following useful

LEMMA 4. *Let $\mathfrak{R} = (r_{kl})$ be a positive definite symmetric matrix and let $\mathfrak{R} = \mathfrak{D}[\mathfrak{G}]$ where $\mathfrak{D}$ is a diagonal matrix with diagonal elements $(d_1, \ldots, d_n)$ satisfying*

$$0 < d_k \leqslant \tau d_{k+1} \qquad (k = 1, \ldots, n-1), \tag{37}$$

and $\mathfrak{G}$ is a triangle matrix all of whose elements are in absolute value $\leqslant \tau$. Then

$$r_1 r_2 \ldots r_n \leqslant \mu(n, \tau)|\mathfrak{R}|, \tag{38}$$

where $\mu(n, \tau)$ depends only on n and τ.

Proof. Since $\mathfrak{R} = \mathfrak{D}[\mathfrak{G}]$ we have

$$r_j = d_j + \sum_{k=1}^{j-1} d_k g_{kj}^2, \tag{39}$$

so that

$$1 \leqslant \frac{r_j}{d_j} \leqslant 1 + \sum_{k=1}^{j-1} \frac{d_k}{d_j} g_{kj}^2 \leqslant c_1(\tau, n). \tag{40}$$

Hence

$$r_1 \ldots r_n \leqslant c_1(\tau, n)^n d_1 \ldots d_n = \mu(n, \tau)|\mathfrak{R}|. \tag{41}$$

Let us now write for our reduced matrix, $\mathfrak{A} = \mathfrak{D}[\mathfrak{G}]$. Since $\mathfrak{A}$ is Minkowski reduced, it follows from the Minkowski reduction theory that $\mathfrak{D}$ and $\mathfrak{G}$ satisfy the conditions of Lemma 4 with $\tau = \tau_n$ depending *only* on n. Since $\mathfrak{A}^{-1} = \mathfrak{D}^{-1}[\mathfrak{G}'^{-1}]$ we get $d_n^{-1} = |\mathfrak{A}_0|/|\mathfrak{A}|$. Using (36) we get

$$d_n \leqslant 2(k/3)^{\frac{1}{2}}. \tag{42}$$

Since $|\mathfrak{A}| = d_1 \ldots d_n$ we get, using (37) and (42), the inequality

$$|\mathfrak{A}| = d_1 \ldots d_n \leqslant (2/\sqrt{3})^n \tau_n^{\frac{1}{2}n(n-1)} k^{\frac{1}{2}n} \tag{43}$$

which gives an upper bound for the "minimum" of a positive abelian form. We are now ready to prove the important

THEOREM 3. *If $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$ is a symplectic reduced positive abelian matrix with kernel k and $\mathfrak{A} = (a_{kl})$, $\mathfrak{C} = (c_{kl})$ then*

$$|\mathfrak{A}||\mathfrak{c}| \leqslant a_1 \ldots a_n c_1 \ldots c_n \leqslant \mu_n|\mathfrak{S}|, \tag{44}$$

μ_n depending only on n.

Proof. Put $\mathfrak{A}^{-1}\mathfrak{B} = -\mathfrak{X}$. Then with the previous notation

$$\mathfrak{S} = \begin{pmatrix} \mathfrak{D} & \mathfrak{O} \\ \mathfrak{O} & k\mathfrak{D}^{-1} \end{pmatrix}\left[\begin{pmatrix} \mathfrak{G} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{G}'^{-1} \end{pmatrix}\begin{pmatrix} \mathfrak{E} & -\mathfrak{X} \\ \mathfrak{O} & \mathfrak{E} \end{pmatrix}\right]; \tag{45}$$

using the matrix $\mathfrak{W}$ which satisfies $\mathfrak{W}^2 = \mathfrak{E}$ we get

$$\mathfrak{S}\begin{bmatrix} \mathfrak{E} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{W} \end{bmatrix} = \begin{pmatrix} \mathfrak{D} & \mathfrak{O} \\ \mathfrak{O} & k\mathfrak{D}^{-1}[\mathfrak{W}] \end{pmatrix}\begin{bmatrix} \mathfrak{G} & -\mathfrak{G}\mathfrak{X}\mathfrak{W} \\ \mathfrak{O} & \mathfrak{W}\mathfrak{G}'^{-1}\mathfrak{W} \end{bmatrix}. \tag{46}$$

In virtue of (42) and Lemma 4, the diagonal matrix and the triangle matrix on the right of (46) satisfy the conditions of Lemma 4. Therefore from the conclusions of that lemma as applied to (46), our theorem follows.

The conditions (32), (34), and (44) are the analogues of those of Gauss for positive binary forms. We can use them to prove

THEOREM 4. *There are only a finite number of integral, positive, symplectic reduced abelian quadratic forms with a given kernel.*

Proof. Let $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$ be a symplectic reduced positive integral abelian matrix. From (34) and (44) we get

$$|\mathfrak{A}| < \mu_n^{\frac{1}{2}} k^{\frac{1}{2}n}. \tag{47}$$

$\mathfrak{A}$ is an integral matrix reduced in the sense of Minkowski. From Minkowski's reduction theory it follows that there are only a finite number of integral $\mathfrak{A}$ satisfying (47). From (32), $\mathfrak{A}^{-1}\mathfrak{B}$ has all its elements between $-\frac{1}{2}$ and $+\frac{1}{2}$. Since $\mathfrak{B}$ is an integral matrix, it follows that there are only finitely many integral $\mathfrak{B}$ satisfying this condition. $\mathfrak{A}\mathfrak{C} - \mathfrak{B}^2 = k\mathfrak{E}$ so that $\mathfrak{C} = \mathfrak{A}^{-1}(k\mathfrak{E} + \mathfrak{B}^2)$, hence when $\mathfrak{A}$ and $\mathfrak{B}$ are known $\mathfrak{C}$ is fixed uniquely. Our contention is thus proved.

In the case $n = 1$ our considerations coincide with those of Gauss and Minkowski. For $n > 1$ it is seen that two symplectically equivalent matrices are equivalent in Minkowski's sense but not necessarily conversely. Also a class of positive integral matrices of determinant k^n (in the sense of Minkowski) may not contain an abelian matrix so that in general we do not have a relation between class number in the symplectic sense and class number in the Minkowski sense. We shall, however, find the symplectic reduced positive quaternary integral abelian forms with a given kernel.

Let us consider positive, integral, abelian, quaternary, quadratic forms of kernel 1 or 2. Let $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$ be a positive abelian matrix of order 4 and kernel $k = 1, 2$. Let $\mathfrak{A} = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ where a, b, c are rational integers and $\mathfrak{A}$ is Minkowski reduced. If $|\mathfrak{A}| = p$ then

$$0 < a \leqslant c, \quad 2b \leqslant a, \quad ac \leqslant 4p/3. \tag{48}$$

Also let $\mathfrak{A} = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$ then $|\mathfrak{A}| = p = d_1 d_2$ and $d_1 = a$. From (42) we get

$$a = d_1 = \frac{p}{d_2} > \frac{p\sqrt{3}}{2\sqrt{k}}.$$

Let us consider two cases, $k = 1$ and 2. In the first case $p < 16/9$ and since p is an integer so $p = 1$. Hence the only symplectic reduced $\mathfrak{S}$ satisfying these conditions is $\mathfrak{A} = \mathfrak{E}_2$, $\mathfrak{B} = \mathfrak{O}$, $\mathfrak{C} = \mathfrak{E}_2$. In the second case $p < 32/9$ or $p = 1, 2$, or 3. When $p = 1$ there is no solution. For $p = 2$, $\mathfrak{A} = \mathfrak{E}_2$, $\mathfrak{B} = \mathfrak{O}$, $\mathfrak{C} = 2\mathfrak{E}_2$ is the only solution. For $p = 3$, $\mathfrak{A} = 2\mathfrak{E}_2$, $\mathfrak{B} = \mathfrak{O}$, $\mathfrak{C} = \mathfrak{E}_2$ is the only solution. But these two solutions are symplectic equivalent. Hence

Integral quaternary positive abelian forms of kernel 1 *or* 2 *constitute each a single class.*

Consider now quaternary positive abelian forms of kernel 3. With the same notation as before we have $p = 1, 2, 3, 4, 5$. If $p = 1$ then $\mathfrak{A} = \mathfrak{E}_2$, $\mathfrak{B} = \mathfrak{O}$, $\mathfrak{C} = 3\mathfrak{E}$ is the only solution. If $p = 2$ then $\mathfrak{A} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, $\mathfrak{B} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $\mathfrak{C} = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}$ is a solution. That these two solutions are not symplectically equivalent is easy to see. For if $\begin{pmatrix} \mathfrak{P} & \mathfrak{Q} \\ \mathfrak{P}_1 & \mathfrak{Q}_1 \end{pmatrix}$ is the transforming modular matrix then

$$\mathfrak{P}'\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\mathfrak{P} + \mathfrak{P}'_1\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\mathfrak{P} + \mathfrak{P}'\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\mathfrak{P}_1 + \mathfrak{P}'_1\begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}\mathfrak{P}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{49}$$

This will mean that $\mathfrak{P}_1 = \mathfrak{O}$ and $\mathfrak{P} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ which contradicts the fact that $\begin{pmatrix} \mathfrak{P} & \mathfrak{Q} \\ \mathfrak{P}_1 & \mathfrak{Q}_1 \end{pmatrix}$ is a modular matrix. Hence

Positive integral abelian quaternary forms of kernel 3 *have at least* 2 *classes represented respectively by* $x_1^2 + x_2^2 + 3x_3^2 + 3x_4^2$ *and* $x_1^2 + 2x_2^2 + 3x_3^2 + 2x_4^2 + 2x_3x_4$.

We can briefly discuss now the reduction theory of indefinite abelian forms. Our method is similar to the usual Hermite method for ordinary quadratic indefinite forms.

Let $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$ be an abelian matrix of kernel k. By Theorem 1 there exists a generalized symplectic matrix $\mathfrak{P}$ such that $\mathfrak{S} = \mathfrak{P}'\mathfrak{D}\,\mathfrak{P}$, where $\mathfrak{D}$ is an abelian diagonal matrix with ± 1 in the diagonal. Put $\mathfrak{H} = \mathfrak{P}'\mathfrak{P}$ so that $\mathfrak{H}$ is a positive abelian matrix with kernel $|k|$. By the considerations above there is a modular matrix $\mathfrak{M}$ such that $\mathfrak{M}'\,\mathfrak{H}\mathfrak{M}$ is symplectic reduced. Let us then call $\mathfrak{M}'\mathfrak{S}\mathfrak{M}$ *symplectic reduced*. It is evident that $\mathfrak{H}$ and $\mathfrak{S}$ satisfy the matrix equation

$$\mathfrak{H}\mathfrak{S}^{-1}\mathfrak{H} = \mathfrak{S}. \tag{50}$$

Let now $\mathfrak{S}[\mathfrak{M}]$ be symplectic reduced. Put $\mathfrak{S}[\mathfrak{M}] = \mathfrak{S}_1$ and $\mathfrak{H}[\mathfrak{M}] = \mathfrak{H}_1$. Then $\mathfrak{H}_1\mathfrak{S}_1^{-1}\mathfrak{H}_1 = \mathfrak{S}_1$. Put now $\mathfrak{H}_2 = \mathfrak{H}_1\begin{bmatrix} \mathfrak{E} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{W} \end{bmatrix}$ and $\mathfrak{S}_2 = \mathfrak{S}_1\begin{bmatrix} \mathfrak{E} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{W} \end{bmatrix}$. Then $\mathfrak{H}_2\mathfrak{S}_2^{-1}\mathfrak{H}_2 = \mathfrak{S}_2$. Furthermore, by (45) and (46), the matrix $\mathfrak{H}_2$ satisfies the condition of

Lemma 4 and hence by a well-known theorem of Siegel there are only a finite number of integral matrices $\mathfrak{S}_2$ with the given kernel k. Thus

THEOREM 5. *There are only a finite number of symplectic reduced integral abelian indefinite matrices with a given kernel.*

It remains now only to point out the geometrical aspect of the problem. In the case of positive binary form $ax^2 + 2bxy + cy^2$, H. J. S. Smith proceeded in the following way. To this positive form associate the complex number $z = a^{-1}(-b + i\sqrt{k})$, where $k = b^2 - ac$, which becomes a point in the upper half of the complex z-plane. The reduction theory of binary forms thus is equivalent to the construction of a fundamental domain for the ordinary modular group. We shall copy this procedure for abelian forms.

Let $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$ be positive real abelian. By the principle of completion of squares we may write

$$\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{O} \\ \mathfrak{O} & k\mathfrak{A}^{-1} \end{pmatrix} \begin{bmatrix} \mathfrak{E} & \mathfrak{A}^{-1}\mathfrak{B} \\ \mathfrak{O} & \mathfrak{E} \end{bmatrix}$$

where $\mathfrak{A}^{-1}\mathfrak{B}$ is symmetric and k is the kernel of $\mathfrak{S}$. Let us put $\mathfrak{A}^{-1}\mathfrak{B} = \mathfrak{X}$ and $\mathfrak{Y} = \sqrt{k}\cdot\mathfrak{A}^{-1}$. Then

$$\mathfrak{S} = \sqrt{k}\begin{pmatrix} \mathfrak{Y}^{-1} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{Y} \end{pmatrix} \begin{bmatrix} \mathfrak{E} & -\mathfrak{X} \\ \mathfrak{O} & \mathfrak{E} \end{bmatrix}.$$

Put $\mathfrak{Z} = \mathfrak{X} + i\mathfrak{Y}$. Then $\mathfrak{Z}$ is a complex symmetric matrix of order n and its imaginary part is the matrix of a positive definite, quadratic form. Thus

$$\mathfrak{Z} = \mathfrak{X} + i\mathfrak{Y} = -\mathfrak{A}^{-1}\mathfrak{B} + i\sqrt{k}\cdot\mathfrak{A}^{-1}$$

is a point of Siegel's half-space of symmetric complex matrices. Because of the presence of the factor $\sqrt{k}$, the correspondence between abelian forms and points in Siegel's half-space is not (1, 1). However, for every point of Siegel's half-space there is a one-parameter family of positive abelian forms, any member of which can be uniquely fixed by its kernel. Thus positive abelian forms can be represented in a (1, 1) way by points in $(n^2 + n + 1)$-dimensional real space. Siegel's space is thus the space of positive abelian forms of kernel unity. His fundamental theorem that the measure of a fundamental domain of the modular group of degree n is finite, is the analogue of Minkowski's result concerning the volume of a fundamental domain on the determinantal surface.

6. Abelian hermitian forms. Another generalization of the theory of binary quadratic forms is the theory of abelian hermitian forms.

Let K_0 be the field of complex numbers. For any matrix $\mathfrak{M}^{(2n)} = \mathfrak{M}$ of $2n$ rows and columns let $\mathfrak{M}^*$ denote the transpose of the complex conjugate of $\mathfrak{M}$. Let $G(K_0,n)$ be the group of matrices $\mathfrak{M}$ with

$$\mathfrak{M}^*\mathfrak{J}\mathfrak{M} = k\mathfrak{J}, \qquad \mathfrak{J} = \begin{pmatrix} \mathfrak{O} & \mathfrak{E} \\ -\mathfrak{E} & \mathfrak{O} \end{pmatrix}, \tag{51}$$

where $k \neq 0$ is a real number. We shall call $G(K_0,n)$ the *generalized h-symplectic*

group. The subgroup $g(K_0,n)$ with $k = \pm 1$ will be called the *h-symplectic group*. If $\mathfrak{M}$ satisfies (51) and $\mathfrak{M} = \mathfrak{M}^*$ we call $\mathfrak{M}$ a *h-abelian matrix*. As before the number k shall be called the *kernel* of the generalized h-symplectic matrix. That h-abelian matrices are generalizations of two by two real symmetric matrices is obvious. For put $n = 1$ and let $\mathfrak{M}$ be positive definite binary hermitian. Put $\mathfrak{M} = \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix}$. From (51) it follows that $b = \bar{b}$ or b is real.

Let R be the field of rational numbers and $d < 0$ a rational integer. Let $R(\sqrt{d})$ be an imaginary quadratic field and let G be the group of matrices $\mathfrak{M}$ with coefficients integral in $R(\sqrt{d})$ and satisfying

$$\mathfrak{M}^*\mathfrak{J}\mathfrak{M} = \mathfrak{J}. \tag{52}$$

G is the *h-modular group* considered recently by Braun. The h-modular group is a generalization of the ordinary 2×2 unimodular group in the rational number field. Braun has shown that for a h-modular matrix $\mathfrak{M}$, $|\mathfrak{M}| = \epsilon^2$ where ϵ is a root of unity in $R(\sqrt{d})$

Let $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}^* & \mathfrak{C} \end{pmatrix}$ be a h-abelian matrix of kernel k and let $\mathfrak{P}$ be h-modular. We call $\mathfrak{S}$ and $\mathfrak{P}^*\mathfrak{S}\mathfrak{P}$, *h-equivalent*. The h-equivalent matrices form a class. We shall sketch very briefly the reduction theory of h-abelian, positive matrices.

Let $\mathfrak{P} = \begin{pmatrix} \mathfrak{P}_1 & \mathfrak{P}_2 \\ \mathfrak{P}_3 & \mathfrak{P}_4 \end{pmatrix}$ run over all h-modular matrices and consider the determinant

$$\left| \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}^* & \mathfrak{C} \end{pmatrix} \begin{Bmatrix} \mathfrak{P}_1 \\ \mathfrak{P}_3 \end{Bmatrix} \right|.$$

We maintain that this has a minimum. This is proved by using the reduction theory of Humbert instead of that of Minkowski. We omit this proof. Let us assume that $\mathfrak{P}$ has been so chosen that $|\mathfrak{A}_1|$ is a minimum, where $\begin{pmatrix} \mathfrak{A}_1 & \mathfrak{B}_1 \\ \mathfrak{B}_1^* & \mathfrak{C}_1 \end{pmatrix} = \mathfrak{S}\{\mathfrak{P}\}$. We can choose $\mathfrak{A}_1$ reduced in the sense of Humbert by multiplying $\mathfrak{P}$ by $\begin{pmatrix} \mathfrak{U} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{U}^{*-1} \end{pmatrix}$ where $\mathfrak{U}$ is a suitable unimodular matrix in $R(\sqrt{d})$. Consider now all modular matrices $\mathfrak{Q} = \begin{pmatrix} \mathfrak{P}_1\mathfrak{U} & \mathfrak{Q}_1 \\ \mathfrak{P}_2\mathfrak{U} & \mathfrak{Q}_2 \end{pmatrix}$. This is obtained from $\mathfrak{P}\begin{pmatrix} \mathfrak{U} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{U}^{*-1} \end{pmatrix}$ by multiplying on the right by $\begin{pmatrix} \mathfrak{E} & \mathfrak{T} \\ \mathfrak{O} & \mathfrak{E} \end{pmatrix}$ where $\mathfrak{T} = \mathfrak{T}^*$ is hermitian and integral in $R(\sqrt{d})$. Let $1, \omega$ be a minimal basis of integers of $R(\sqrt{d})$. Every complex number can be uniquely written in the form $a + b\omega$ where a and b are real. Write $\mathfrak{T} = \mathfrak{T}_1 + \omega\mathfrak{T}_2$ where $\mathfrak{T}_1$ and $\mathfrak{T}_2$ are rational integral matrices. Let

$$\mathfrak{S}\left\{\mathfrak{P}\begin{pmatrix} \mathfrak{U} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{U}^{*-1} \end{pmatrix}\begin{pmatrix} \mathfrak{E} & \mathfrak{T} \\ \mathfrak{O} & \mathfrak{E} \end{pmatrix}\right\} = \begin{pmatrix} \mathfrak{A}_2 & \mathfrak{B}_2 \\ \mathfrak{B}_2^* & \mathfrak{C}_2 \end{pmatrix}.$$

Then $\mathfrak{A}_2^{-1}\mathfrak{B}_2$ is hermitian and can be written as $\mathfrak{F}_1 + \omega\mathfrak{F}_2$ where $\mathfrak{F}_1$ and $\mathfrak{F}_2$ are real. Choose now $\mathfrak{T}$ in such a way that $\mathfrak{F}_1 + \mathfrak{T}_1$ and $\mathfrak{F}_2 + \mathfrak{T}_2$ have all elements

between $-\frac{1}{2}$ and $+\frac{1}{2}$. We shall call $\begin{pmatrix} \mathfrak{A}_2 & \mathfrak{B}_2 \\ \mathfrak{B}_2^* & \mathfrak{C}_2 \end{pmatrix}$ a *h-symplectic reduced matrix*. Thus if $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}^* & \mathfrak{C} \end{pmatrix}$ is a h-symplectic reduced h-abelian matrix, then

(53) (i) $|\mathfrak{A}|$ is minimum,
(ii) $\mathfrak{A}$ is reduced in the sense of Humbert,
(iii) $\mathfrak{A}^{-1}\mathfrak{B} = \mathfrak{F}_1 + \omega\mathfrak{F}_2$ is such that $\mathfrak{F}_1$ and $\mathfrak{F}_2$ have all their elements in the interval $(-\frac{1}{2}, \frac{1}{2})$.

It is thus evident, as a first result, that

$$|\mathfrak{C}| > |\mathfrak{A}|. \tag{54}$$

By a known theorem of Humbert, there exists an integral matrix $\mathfrak{A}_p$ determined by the integer n and the field $R(\sqrt{d})$ such that $\mathfrak{A}\{\mathfrak{A}_p\} = \mathfrak{D}\{\mathfrak{L}\}$ where $\mathfrak{D}$ is a diagonal matrix and $\mathfrak{L}$ is a triangle matrix satisfying conditions similar to Lemma 4. We therefore see, in virtue of a lemma of H. Braun's, that the matrix

$$\begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}^* & \mathfrak{C} \end{pmatrix}\begin{Bmatrix} \mathfrak{A}_p & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{A}_p{}^{*-1}\mathfrak{W} \end{Bmatrix} = \begin{pmatrix} \mathfrak{D} & \mathfrak{O} \\ \mathfrak{O} & k\mathfrak{D}^{-1}\{\mathfrak{W}\} \end{pmatrix}\begin{Bmatrix} \mathfrak{L} & \mathfrak{L}\mathfrak{A}_p{}^{-1}\mathfrak{X}\mathfrak{A}_p{}^{*-1}\mathfrak{W} \\ 0 & \mathfrak{W}\mathfrak{L}\mathfrak{W} \end{Bmatrix} \tag{55}$$

satisfies conditions like those in Lemma 4. Here $\mathfrak{X} = -\mathfrak{A}^{-1}\mathfrak{B}$. Therefore from Humbert's results we get

$$|\mathfrak{A}\{\mathfrak{A}_p\}|\,|\mathfrak{C}\{\mathfrak{A}_p{}^{*-1}\mathfrak{W}\}| < \mu_n k^n, \tag{56}$$

where μ_n depends only on n and d. Thus we have the important

THEOREM 6. *An h-reduced h-abelian positive matrix* $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}^* & \mathfrak{C} \end{pmatrix}$ *satisfies*

$$0 < |\mathfrak{A}| < |\mathfrak{C}|, \quad |\mathfrak{A}|\,|\mathfrak{C}| < \mu_n k^n, \quad \mathfrak{A}^{-1}\mathfrak{B} = \mathfrak{F}_1 + \omega\mathfrak{F}_2, \tag{57}$$

where μ_n *depends only on* n *and* d, *and* $\mathfrak{F}_1$ *and* $\mathfrak{F}_2$ *have all their elements in the interval* $(-\frac{1}{2}, \frac{1}{2})$.

It is now a simple matter to prove that positive h-abelian integral matrices of a given kernel have only finitely many classes. To extend this to integral indefinite forms use has to be made of Theorem 1′. These considerations are simple and we omit them.

A geometric representation for positive h-abelian forms is possible. As before we write

$$\begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}^* & \mathfrak{C} \end{pmatrix} = \begin{pmatrix} \mathfrak{A} & \mathfrak{O} \\ \mathfrak{O} & k\mathfrak{A}^{-1} \end{pmatrix}\begin{Bmatrix} \mathfrak{E} & \mathfrak{A}^{-1}\mathfrak{B} \\ \mathfrak{O} & \mathfrak{E} \end{Bmatrix} = \sqrt{k}\begin{pmatrix} \mathfrak{Y}^{-1} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{Y} \end{pmatrix}\begin{Bmatrix} \mathfrak{E} & -\mathfrak{X} \\ \mathfrak{O} & \mathfrak{E} \end{Bmatrix}, \tag{58}$$

where $\mathfrak{Y} = \sqrt{k}\cdot\mathfrak{A}^{-1}$, $\mathfrak{X} = -\mathfrak{A}^{-1}\mathfrak{B}$. Now $\mathfrak{Y}$ is positive hermitian. Put $\mathfrak{Z} = \mathfrak{X} + i\,\mathfrak{Y}$; then $\mathfrak{Z}$ is a complex matrix of order n and $\mathfrak{Y} = (\mathfrak{Z} - \mathfrak{Z}^*)/2i$ is positive hermitian. This space is also a generalization of the usual upper half of the complex z-plane in the same way as Siegel's. Thus positive h-abelian forms can be represented in a $(1, 1)$ way by points in a $(2n^2 + 1)$-dimensional real space.

It can also be seen that the space of complex matrices $\mathfrak{Z}$ with $(\mathfrak{Z} - \mathfrak{Z}^*)/2i$ positive hermitian is the space corresponding to the hermitian matrix $\mathfrak{T} = \sqrt{d}\begin{pmatrix} \mathfrak{D} & \mathfrak{E} \\ -\mathfrak{E} & \mathfrak{D} \end{pmatrix}$. The h-modular group is the unit group of $\mathfrak{T}$. The reduction theory of positive h-abelian matrices corresponds to construction of a fundamental domain in the $\mathfrak{Z}$-space for the units of $\mathfrak{T}$. The $\mathfrak{Z}$-space is thus the space of positive h-abelian forms of kernel 1. From [8] it follows that a fundamental domain in the $\mathfrak{Z}$-space for the h-modular group has a finite measure, in terms of the invariant measure in this homogeneous space. Since $\mathfrak{T}$ can represent zero non-trivially, this fundamental domain is not compact.

7. Generalizations. Siegel's considerations in [11] show that the positive abelian forms we have considered can be viewed as constituting homogeneous spaces of cosets G/C of a certain Lie group G by a closed maximal compact subgroup C. The reduction theory of positive abelian forms is equivalent to construction of fundamental domains for certain discrete groups H (the modular group and the h-modular group) acting in these spaces. Minkowski's reduction theory concerns the case where G is the full linear group, C is the orthogonal group, and H is the ordinary unimodular group. These ideas suggest that analogous results might be obtained by considering other types of coset spaces. We shall consider a simple example.

Let G be the group of complex matrices $\mathfrak{C}$ satisfying

$$\mathfrak{C}'\mathfrak{C} = k\mathfrak{E}, \tag{59}$$

$\mathfrak{E} = \mathfrak{E}_n$, and $k \neq 0$ a real number. The real orthogonal group g is a maximal, compact subgroup of G and the coset space G/g is homeomorphic to the space of positive hermitian matrices $\mathfrak{H}$ which satisfy (59). A little calculation shows that every positive hermitian matrix $\mathfrak{H}$ satisfying (59) has the parametric representation

$$\mathfrak{H} = \sqrt{k}\cdot(\mathfrak{E} - i\mathfrak{Y})(\mathfrak{E} + i\mathfrak{Y})^{-1}, \tag{60}$$

where $\mathfrak{Y}$ is a skew symmetric real matrix of order n satisfying $\mathfrak{E} + \mathfrak{Y}^2 > 0$. Let $n > 4$ and H the group of matrices $\mathfrak{C}$ whose elements are Gaussian integers and satisfying

$$\mathfrak{C}'\mathfrak{C} = \mathfrak{E}. \tag{61}$$

This is an infinite group and is a discrete subgroup of G. If $\mathfrak{S}_1$ and $\mathfrak{S}_2$ are hermitian (not necessarily positive) in G we say that $\mathfrak{S}_1$ and $\mathfrak{S}_2$ are *equivalent* if for a matrix $\mathfrak{C}$ in H the relation $\mathfrak{S}_1 = \mathfrak{S}_2\{\mathfrak{C}\}$ holds. All equivalent hermitian matrices fall into a class. To obtain a reduction theory of positive hermitian matrices in G we proceed thus.

Let H_0 be the space of all positive hermitian matrices which are orthogonal. Let R_0 be the space of Humbert reduced positive hermitian matrices of determinant 1. Let Ω be the group of $n \times n$ matrices whose elements are Gaussian integers and whose determinant is ± 1. Let $\mathfrak{C}_1, \mathfrak{C}_2, \ldots$ be representatives of cosets of Ω/H. It can be seen as a simple consequence of Humbert's theory that

only finitely many $\mathfrak{C}_1, \mathfrak{C}_2, \ldots$ are such that $R_0(\mathfrak{C}_k^{-1})$ intersects H_0 in a non-empty set. Let $H_k = R_0(\mathfrak{C}_k^{-1}) \cap H_0$ and let

$$F = \sum_k (R_0(\mathfrak{C}_k^{-1}) \cap H_0).$$

Then F is a fundamental domain for H in H_0. Since $n > 4$, this fundamental domain F is non-compact but has a finite measure, in terms of the invariant measure in H. It can be proved that the invariant volume measure is

$$dV = |\mathfrak{E} + \mathfrak{Y}^2|^{\frac{1}{2}(1-n)}\{d\mathfrak{Y}\},$$

where $\{d\,\mathfrak{Y}\}$ is the Euclidean volume element in the space $\mathfrak{E} + \mathfrak{Y}^2 > 0$.

Let now $\mathfrak{S}$ in G be positive hermitian. To each $\mathfrak{S}$ associate a $\mathfrak{S}_1$ such that

$$\sqrt{k}\,\mathfrak{S}_1 = \mathfrak{S}. \tag{62}$$

Then $\mathfrak{S}_1$ is a point of H_0. Choose $\mathfrak{C}$ in H in such a way that $\mathfrak{S}_1\{\mathfrak{C}\}$ is in F. We then call $\mathfrak{S}\{\mathfrak{C}\}$ *reduced*. It can then be deduced as a consequence of Humberts' reduction theory that there are only a finite number of classes of integral (Gaussian integers) positive hermitian $\mathfrak{S}$ with a given k. A consequence of this reduction theory is that H has a finite number of generators.

References

1. H. Braun, *Hermitian modular functions* III, Ann. Math., vol. 53 (1951), 143-160.
2. C. Chevalley, *Theory of Lie groups* I (Princeton, 1946).
3. G. Cotty, *Les fonctions abéliennes et la théorie des nombres*, Ann. Fac. Sci. Toulouse, ser. 3, vol. 3 (1911), 209-376.
4. C. Hermite, *Sur la théorie de la transformation des fonctions abéliennes*, Oeuvres, vol. 1 (Paris, 1905), 444-478.
5. P. Humbert, *Réduction de formes quadratiques dans un corps algébrique fini*, Comment. Math. Helv., vol. 23 (1949), 50-63.
6. F. Klein and R. Fricke, *Vorlesungen über die Theorie der Modul-Funktionen*, vol. 1 (Leipzig, 1890), 243-269.
7. E. Laguerre, *Sur le calcul des systèmes linéaires*, Oeuvres, vol. 1 (Paris, 1898), 221-267.
8. K. G. Ramanathan, *The theory of units of quadratic and hermitian forms*, Amer. J. Math., vol. 73 (1951), 233-255.
9. C. L. Siegel, *Einheiten quadratischer Formen*, Abh. Sem. Hansischen Univ., vol. 13 (1939), 209-239.
10. ———, *Symplectic geometry*, Amer. J. Math., vol. 65 (1943), 1-86.
11. ———, *Some remarks on discontinuous groups*, Ann. Math., vol. 46 (1945), 708-718.
12. B. L. van der Waerden, *Moderne Algebra*, vol. 1 (Berlin, 1930).

Tata Institute for Fundamental Research

GROUPS WITH A CERTAIN CONDITION ON CONJUGATES

FRANKLIN HAIMO

1. Introduction. In this paper, we shall show that if $\mathfrak{G}$ is a nilpotent [5] group and if M, a positive integer, is a uniform bound on the number of conjugates that any element of $\mathfrak{G}$ may have, then there exist "large" integers n for which $x \to x^n$ is a central endomorphism of $\mathfrak{G}$. If $\mathfrak{G}$ is not necessarily nilpotent, if the above condition on the conjugates is retained, and if we can find a member of the lower central series [1], every element of which lies in some member of the ascending central series, then we shall show that every non-unity element of the "high" derivatives has finite order.

2. Commutator relations. In a group $\mathfrak{G}$, let $(x, y) = xyx^{-1}y^{-1}$. In general, commutator notation is to be that of [5]. Let $\{x, y\}$ be that subgroup of $\mathfrak{G}$ which has generators x and y. By $\mathfrak{T} = \mathfrak{T}(x, y)$ we mean[1] the smallest normal subgroup of $\{x, y\}$ which contains both $((x, y), x)$ and $((x, y), y)$. If (x, y) commutes with both x and y, then

$$(x, y)^n = (x^n, y) = (x, y^n),$$

for every positive integer n, as an induction will show. Similarly

$$(xy)^n = x^n y^n (y, x)^\theta \qquad (\theta = \tfrac{1}{2}n(n-1)).$$

In $\{x, y\}/\mathfrak{T}$, $(x, y)\mathfrak{T}$ commutes with $x\mathfrak{T}$ and $y\mathfrak{T}$. Hence the above commutator formulae can be modified to $(x, y)^n \equiv (x^n, y) \equiv (x, y^n) \bmod \mathfrak{T}(x, y)$ and to $(xy)^n \equiv x^n y^n (y, x)^\theta \bmod \mathfrak{T}(x, y)$ for every $x, y \in \mathfrak{G}$.

3. The uniform bound. In this section, we assume that $\mathfrak{G}$ is a non-trivial group and that M is a positive integer such that the number of conjugates for any element $x \in \mathfrak{G}$ cannot exceed M. We shall call such a group a u.b. group, or say that the group is u.b.; M will be called the u.b. of $\mathfrak{G}$. Let $\mathfrak{Z}^{(1)}$ be the centre of $\mathfrak{G}$. Suppose that $\mathfrak{Z}^{(i)}$ is defined. Then $\mathfrak{Z}^{(i+1)}$ is to be that subgroup of $\mathfrak{G}$ for which $\mathfrak{Z}^{(i+1)}/\mathfrak{Z}^{(i)}$ is the centre of $\mathfrak{G}/\mathfrak{Z}^{(i)}$, and we have described the ascending central series [1] of $\mathfrak{G}$. We say that a group is a *torsion group* if every non-unity element thereof has finite order. If every element of a group $\mathfrak{G}$ has infinite order, we say that the group is *torsion-free*.

The group $\mathfrak{G}$ is said to have *uniform torsion* and is called u.t. if there exists a positive integer α such that $x^\alpha = 1$ for all $x \in \mathfrak{G}$; α might be called the *exponent*

Received April 3, 1951; in revised form October 11, 1951. Presented to the American Mathematical Society, November 25, 1950.

[1]The proof of the principal result has been simplified as suggested by the referee, whereby properties of the $\mathfrak{G}/\mathfrak{T}$ are used.

of $\mathfrak{G}$. If $\mathfrak{G}$ is u.b. with bound M then $\mathfrak{G}/\mathfrak{Z}^{(1)}$ is u.t. with exponent $\mathfrak{a}$ dividing $M!$ For, if $g, h \in \mathfrak{G}$, the set

$$\{h^{-i}gh^{i}\} \qquad (i = 0, 1, 2, \ldots, M)$$

cannot have $M+1$ distinct elements. Equating a suitable pair of these, we find an integer m, $1 \leqslant m \leqslant M$, such that $h^{m}g = gh^{m}$. Now $m \mid M! = \mu$ so that $h^{\mu}g = gh^{\mu}$. The result is well known. For later use, we recall the fact that, for any group $\mathfrak{G}$ and positive integer i,

$$(\mathfrak{G}, \mathfrak{Z}^{(i+1)}) \subset \mathfrak{Z}^{(i)}.$$

Suppose that $\mathfrak{G}/\mathfrak{Z}^{(1)}$ is u.t. with exponent $\mathfrak{a}$ and that $\mathfrak{N}$ is any normal subgroup of $\mathfrak{G}$. For $x \in \mathfrak{G}$, $y \in N$, $\mathfrak{T}(x, y) \subset (\mathfrak{G}, (\mathfrak{G}, \mathfrak{N}))$ so that

$$(x, y)^{\mathfrak{a}} \equiv (x^{\mathfrak{a}}, y) \equiv 1 \qquad \text{mod } (\mathfrak{G}, (\mathfrak{G}, \mathfrak{N})),$$

by the first of the commutator relations above. Let $\mathfrak{S}$ be the set of all $s \in (\mathfrak{G}, \mathfrak{N})$ for which $s^{\mathfrak{a}} \in (\mathfrak{G}, (\mathfrak{G}, \mathfrak{N}))$. Then the members of $\mathfrak{S}$ form a set of generators for $(\mathfrak{G}, \mathfrak{N})$, and $\mathfrak{S}$ contains the inverse of each of its elements. Now let s and t be elements of $\mathfrak{S}$. Then

$$(s, t) \in ((\mathfrak{G}, \mathfrak{N}), (\mathfrak{G}, \mathfrak{N})) \subset (\mathfrak{G}, (\mathfrak{G}, \mathfrak{N})).$$

By the second of the commutator relations, $(st)^{\mathfrak{a}} \equiv 1 \bmod (\mathfrak{G}, (\mathfrak{G}, \mathfrak{N}))$, and $\mathfrak{S} = (\mathfrak{G}, \mathfrak{N})$. We have the proof of the first part of the following

LEMMA. $(\mathfrak{G}, \mathfrak{N})/(\mathfrak{G}, (\mathfrak{G}, \mathfrak{N}))$ *is* u.t. *with exponent dividing* $\mathfrak{a}$ *whenever* $\mathfrak{G}/\mathfrak{Z}^{(1)}$ *is* u.t. *with exponent* $\mathfrak{a}$ *and* $\mathfrak{N}$ *is a normal subgroup of* $\mathfrak{G}$; $(\mathfrak{G}, \mathfrak{Z}^{(i+1)})$ *is* u.t. *with exponent* $\mathfrak{a}(i)$, *where* $\mathfrak{a}(i) \mid \mathfrak{a}^{i}$ *and where* $\mathfrak{a}(i) \mid \mathfrak{a}(i+1)$.

That $\mathfrak{a}(i) \mid \mathfrak{a}(i+1)$ is obvious. To show that $\mathfrak{a}(i) \mid \mathfrak{a}^{i}$, we note that the result holds if $i = 0$; and if it holds for $i = k-1$, take $\mathfrak{N}$ above to be $\mathfrak{Z}^{(k+1)}$. Then $(\mathfrak{G}, \mathfrak{N}) \subset \mathfrak{Z}^{(k)}$, and

$$(\mathfrak{G}, \mathfrak{Z}^{(k+1)})/[(\mathfrak{G}, \mathfrak{Z}^{(k)}) \cap (\mathfrak{G}, \mathfrak{Z}^{(k+1)})]$$

is u.t. with exponent dividing $\mathfrak{a}$. Hence $(\mathfrak{G}, \mathfrak{Z}^{(k+1)})$ is u.t. with exponent $\mathfrak{a}(k)$ where $\mathfrak{a}(k) \mid \mathfrak{a} \,.\, \mathfrak{a}(k-1)$. The induction assumption includes $\mathfrak{a}(k-1) \mid \mathfrak{a}^{(k-1)}$, so that $\mathfrak{a}(k) \mid \mathfrak{a}^{k}$.

THEOREM. *If* $\mathfrak{G}/\mathfrak{Z}^{(1)}$ *is* u.t. *and if* $\gamma(i) = \mathfrak{a} \,.\, \mathfrak{a}(i-1)$ (*where* $\mathfrak{a}(i-1)$ *is the exponent of* $(\mathfrak{G}, \mathfrak{Z}^{(i)})$), *then the mapping* $x \to x^{\gamma(i)}$ *on* $\mathfrak{G}$ *induces an endomorphism of* $\mathfrak{Z}^{(i)}$ *into* $\mathfrak{Z}^{(1)}$.

Proof. If $x, y \in \mathfrak{Z}^{(i)}$, $(xy)^{\mathfrak{a}} = x^{\mathfrak{a}} y^{\mathfrak{a}} z$, where

$$z \in (\mathfrak{Z}^{(i)}, \mathfrak{Z}^{(i)}) \cap \mathfrak{Z}^{(1)} \subset (\mathfrak{G}, \mathfrak{Z}^{(i)}) \cap \mathfrak{Z}^{(1)}.$$

Hence $(xy)^{\gamma(i)} = x^{\gamma(i)} y^{\gamma(i)}$. For, $z \in (\mathfrak{Z}^{(i)}, \mathfrak{Z}^{(i)})$ by the second of the commutator relations, using the fact that $\mathfrak{T}(x, y) \subset (\mathfrak{Z}^{(i)}, \mathfrak{Z}^{(i)})$; and $z \in \mathfrak{Z}^{(1)}$, since $w^{\mathfrak{a}} \in \mathfrak{Z}^{(1)}$ for every $w \in \mathfrak{G}$. Since $(\mathfrak{G}, \mathfrak{Z}^{(i)})$ is u.t. with exponent $\mathfrak{a}(i-1)$, $\gamma(i)$ has the indicated property.

4. The consequences of the theorem.

COROLLARY 1. *Let* $\mathfrak{G}/\mathfrak{Z}^{(1)}$ *be* u.t., *and let* $\mathfrak{G}$ *be nilpotent of class* c. *Then the mapping* $x \to x^{v(c)}$ *is a central endomorphism of* $\mathfrak{G}$.

Proof. Take $i = c$ in the theorem.

COROLLARY 2. *If* $\mathfrak{G}/\mathfrak{Z}^{(1)}$ *is* u.t. *and if any member of the ascending central series is torsion-free, then the ascending central series collapses and contains only the centre.*

Proof. If $\mathfrak{Z}^{(n)}$ is torsion-free and if $g \in \mathfrak{Z}^{(n+1)}$, $n \geqslant 1$, then

$$gxg^{-1}x^{-1} \in (\mathfrak{G}, \mathfrak{Z}^{(n+1)}) \subset \mathfrak{Z}^{(n)}$$

for every $x \in \mathfrak{G}$, and the u.t. property of $(\mathfrak{G}, \mathfrak{Z}^{(n+1)})$ shows that $gxg^{-1}x^{-1} = 1$, the unity of $\mathfrak{G}$. Then $gx = xg$ for every $x \in \mathfrak{G}$, and $\mathfrak{Z}^{(n+1)} \subset \mathfrak{Z}^{(1)}$.

COROLLARY 3. *A non-Abelian nilpotent group* $\mathfrak{G}$ *with torsion-free centre cannot be* u.b.

For a given group $\mathfrak{G}$ let $\mathfrak{Z} = \mathfrak{Z}(\mathfrak{G})$ be the set sum of the $\mathfrak{Z}^{(i)}$ $(i = 1, 2, 3, \ldots)$. $\mathfrak{Z}$ is a normal subgroup of $\mathfrak{G}$; and $\mathfrak{G} = \mathfrak{Z}$ if $\mathfrak{G}$ is nilpotent. The converse of the latter statement need not hold. If $\mathfrak{G} = \mathfrak{Z}$ we call $\mathfrak{G}$ *weakly nilpotent*. From the principal theorem, if $\mathfrak{G}/\mathfrak{Z}^{(1)}$ is u.t., then $(\mathfrak{G}, \mathfrak{Z})$ is a torsion subgroup of $\mathfrak{G}$. Similarly, we have the following results:

LEMMA. *If* $\mathfrak{G}/\mathfrak{Z}^{(1)}$ *is* u.t.[2] *and if* $\mathfrak{G}$ *is weakly nilpotent, then* $(\mathfrak{G}, \mathfrak{G})$ *is a torsion subgroup of* $\mathfrak{G}$.

LEMMA. *If* $\mathfrak{G}/\mathfrak{Z}^{(1)}$ *is* u.t. *and if* $\mathfrak{Z} \supset {}^{k}\mathfrak{G}$, *a member of the lower central series of* $\mathfrak{G}$, *then* (a) *the* ${}^{k+2}\mathfrak{G}$, $k > 0$, *are torsion subgroups; and* (b) *for "large"* j, *the* $\mathfrak{G}^{(j)}$, *members of the derived series are torsion subgroups.*

Proof. (See [5] and [1] for definitions.) (a) $\mathfrak{Z} \supset {}^{k}\mathfrak{G}$ implies

$$(\mathfrak{G}, \mathfrak{Z}) \supset (\mathfrak{G}, {}^{k}\mathfrak{G}) = {}^{k+1}\mathfrak{G} \supset {}^{k+2}\mathfrak{G} \qquad (k > 2).$$

(b) It is known [1] that $\mathfrak{G}^{(j)} \subset {}^{k}\mathfrak{G}$ $(k = 2^j - 1)$. Choose $j \geqslant \log_2(i + 2)$ for the desired result.

It is well known [3] that the integers n for which $x \to x^n$ is a central endomorphism form an ideal. It would be of interest to extend the work of Levi and van der Waerden and of Bruck [2], concerning central endomorphisms of the form $x \to x^3$, to the general central power endomorphism. But the methods, as in [2], seem to depend on the fact that 3 is "small."

[2] For a related result when $\mathfrak{G}$ is u.b. see [4].

References

1. R. Baer, *The higher commutator subgroups of a group*, Bull. Amer. Math. Soc., vol. 50 (1944), 143-160.
2. R. H. Bruck, *Contributions to the theory of loops*, Trans. Amer. Math. Soc., vol. 60 (1946), 245-354.
3. F. W. Levi, *Notes on group theory* VII, J. Indian Math. Soc. (N.S.), vol. 9 (1945), 37-42 (as available in Math. Rev., vol. 8 (1947), 13).
4. B. H. Neumann, *Groups with finite classes of conjugate elements*, Proc. London Math. Soc. (3), vol. 1 (1951), 178-187.
5. H. Zassenhaus, *Lehrbuch der Gruppentheorie* (Leipzig and Berlin, 1937).

Washington University in Saint Louis

ON A CONJECTURE BY J. H. CHUNG

G. DE B. ROBINSON

1. Introduction. The present paper is a sequel to that of J. H. Chung (**2**) and contains a proof of a conjecture made by him, namely, that *the number of ordinary (modular) irreducible representations contained in a given p-block of S_n is independent of the p-core.* A summary of the results contained herein appeared in the Proceedings of the National Academy of Sciences (**9**).

The Main Theorem on which the proof of the conjecture depends is of some interest. It was stated without proof by Nakayama and Osima (**6**, p. 115) and obtained independently by the author (**9**). It has been known for some time that the p-hook structure of a Young diagram $[\alpha]$ is given by a certain star diagram (**7**; also **6**, **9**, **10**, **11**), with each of whose p disjoint constituents can be associated a unique residue class modulo p. What was not realized is that the converse theorem is also valid. The first part of Chung's conjecture concerning ordinary representations follows immediately from this theorem, while the proof of the second part concerning modular representations requires a detailed study of the independence of Chung's identities which are satisfied by the rows of the decomposition matrix $D = (d_{ij})$.

Note added April 1, 1952. Since the writing of the present paper the problem of the modular representations of the symmetric group has been approached from a fresh point of view by D. E. Littlewood (Proc. Royal Soc. (London), (A), vol. 209 (1951), 333-353) and the present author (Proc. Nat. Acad. Sci., vol. 38 (1952), 129-133; 424-426). Chung's characterization of an indecomposable has been made explicit, while new light has been thrown on the modular irreducible representations themselves. So far as the contents of this paper is concerned, the new approach associates a residue (mod p) with *each* node of a disjoint constituent of the star diagram rather than with the upper left-hand corner node only, but the proof of the Main Theorem is largely unaffected.

2. The Main Theorem. The notion of a p-hook was introduced by Nakayama (**4**) and has proved most fruitful in studying the modular representation theory of the symmetric group S_n. If as many p-hooks as possible are removed from a diagram $[\alpha]$ containing n nodes, then the residue $[\alpha_0]$ is called the *p-core* of $[\alpha]$ and we have the basic theorem of the modular theory (**4**, p. 423; **1**; **6**):

2.1. *Two irreducible representations $[\alpha]$ and $[\beta]$ of S_n belong to the same p-block if and only if they have the same p-core.*

To proceed further it is necessary to know something of the p-hook structure of $[\alpha]$, i.e., of the star diagram $[\alpha]^*$ of $[\alpha]$. If b p-hooks are removable from $[\alpha]$

Received September 12, 1951.

we shall say (9) that $[a]$ is of *weight* b. We shall write

$$[a]_p^* = [\lambda_0]\cdot[\lambda_1]\cdot \ldots \cdot[\lambda_{p-1}], \tag{2.2}$$

where the $[\lambda_r]$ are the disjoint right constituents of $[a]^*$ which are determined explicitly in terms of the p-chains (7; 10) of $[a]$. We assume that $[\lambda_r]$ contains b_r nodes, where

$$b = b_0 + b_1 + \ldots + b_{p-1}, \tag{2.3}$$

and r is the leg length of the p-hook represented by its upper left-hand corner node. We shall call r the *class* of the constituent $[\lambda_r]$. We prove the following

2.4. MAIN THEOREM. *A diagram* $[a]$ *of weight* b *exists and is uniquely determined by assigning*:

(i) *its* p*-core* $[a_0]$;
(ii) *its star diagram* $[a]^*$;
(iii) *the class of each disjoint constituent* $[\lambda_r]$.

As a preliminary to the proof it is necessary to remind the reader of a fundamental result of Young which can be stated in the form (7, p. 283)

$$[a] = \sum [a'], \tag{2.5}$$

where $[a']$ is obtained by removing a node from $[a]$, and the summation indicates that this is to be done in all possible ways. From a group-theoretic point of view, the equation 2.5 gives the reduction of $[a]$ when S_n is restricted to the subgroup S_{n-1}. It is convenient to describe this process of removing a node as *differentiating* $[a]$; conversely, we may speak of $[a]$ as the *integral* of the set of $[a']$'s (2, p. 337; 3).

Proof. (a) *Suppose first that* $[a]^*$ *has just one constituent* $[\lambda]$ *and it is of class* r. Certainly the theorem is true for $b = 1$, as was shown by Nakayama (4) and Chung (2); we shall assume it to be true for all diagrams of weight less than $b > 1$ and prove it for diagrams $[a]$ of weight b. Let us differentiate $[\lambda]$, obtaining a derived set $[\lambda']_i$, where $i = 1, 2, \ldots, k$.

Assume that $k > 1$. Clearly the class of each $[\lambda']_i$ is also r, since this depends on the last p-hook removable, i.e., on the upper left-hand corner node of $[\lambda]$. By our inductive assumption, a unique diagram $[a']_i$ is associated with each such $[\lambda']_i$ of class r. Since each node removable from $[\lambda]$ belongs to the same constituent, these nodes represent (4, §§4, 5; 7, p. 288) non-overlapping p-hooks of $[a]$. Thus each $[a']_i$ can be obtained by adding $k - 1$ non-overlapping p-hooks to a certain diagram $[\bar{a}]$ which is the residue left when all k p-hooks are removed from $[a]$. Considering the set of k diagrams $[a']_i$ together, it follows that the k p-hooks can be added simultaneously to $[\bar{a}]$ to yield $[a]$. The uniqueness of $[a]$ is thus proved for $k \geqslant 2$.

Assume that $k = 1$. In this case we know that $[\lambda]$ must be of the form $[x^y]$. Again by our inductive hypothesis, we know that a unique diagram exists having

as star diagram $[\bar{\lambda}] = [(x-1)^{p-1}]$. Such a diagram is an $(x+y-1)p$-core,[1] since $[(x-1)^{p-1}]$ is an $(x+y-1)$-core, and so there can be added to this core an $(x+y-1)p$-hook chosen so as to have the desired representation $[\lambda] - [\bar{\lambda}]$, of class r. This completes the proof of the theorem in case (a).

(b) *If* $[\alpha]^*$ *has more than one constituent* $[\lambda]$, we may again consider the set of k derived diagrams which we can divide into at most p subsets with k_r ($r = 0, 1, \ldots, p-1$) diagrams in the rth set which differ only in the constituent of class r.

Assume that $k_r > 1$ *and* $k_s > 1$. The argument of case (a) is applicable to the rth set and we obtain a unique diagram $[\alpha^r]$. Similarly, we obtain a unique diagram $[\alpha^s]$ from the sth set. In order to prove that $[\alpha^r] = [\alpha^s]$ we note that the two diagrams can differ only in the positions of at most two p-hooks, in view of our inductive assumption; and each of these can be added separately to a common part $[\alpha_1]$ in a unique manner. If these added p-hooks do not overlap then certainly $[\alpha^r] = [\alpha^s]$. If they do overlap, they can be added in succession, the resulting diagram being obtained (**4**, §3) by moving the common part down and to the right one place, leaving the non-overlapping parts in their original positions. Thus again, $[\alpha^r] = [\alpha^s]$.

The extension of the argument to the case where one or more of the k_r's is unity presents no added difficulty, and after at most p steps the theorem is proved in case (b) also.

It is to be noted that the conditions (i), (ii), (iii) in the above theorem are independent. The significance of (i) has already been seen in 2.1. With regard to (ii) and (iii), it is clear that each partition 2.3 of b leads to a class of star diagrams and the number of diagrams in each class depends again on the number of partitions of each b_r. It is also evident that each b_r is to be associated with a residue class r modulo p, and the number of representations belonging to a given block will depend on the number of ways this association can be made. To sum up, we have the following corollary of the Main Theorem:

2.6. *The number* ρ *of ordinary irreducible representations in any* p*-block of weight* b *is independent of the* p*-core and is determined by the conditions* (ii) *and* (iii), *i.e., by the number of possible star diagrams and the number of different ways the* p *distinct residue classes can be associated with the disjoint constituents.*

3. Chung's identities between the rows of D. In the general modular theory the splitting of an ordinary irreducible representation of a finite group G into its modular components is given by the decomposition matrix $D = (d_{ij})$. If we suppose the representations arranged in blocks B_k, the matrix D takes the form

[1] Nakayama's original theorem (**5**, p. 414) was phrased so as to apply to hooks of prime length p, but it and the hook structure theorem (**7**, p. 287) defining the star diagram, as well as the converse being proved here, are all valid for hooks of composite length. The argument at this point in the proof requires just this generality.

3.1
$$\begin{pmatrix} D_1 D_2 & & 0 \\ & \cdots & \\ 0 & & D_\omega \end{pmatrix},$$

where the reduction of the representations belonging to B_k is given by D_k. For the symmetric group this arrangement is easy to achieve in view of 2.1.

Since the indecomposable representations of the regular representation of G, or alternatively, the modular representations of G belonging to B_k, are associated with the columns of D_k, it follows that there will be a set of identities holding between the rows of D_k. The number of these identities for D as a whole is $\rho - \sigma$, where ρ is the number of classes of G and σ is the number of these which are p-regular. *Thus $\rho - \sigma$ is equal to the number of p-singular classes of G.* If we denote by ρ_k the number of ordinary irreducible representations in the block B_k, and by σ_k the number of indecomposables of B_k, then we have

3.2
$$\rho - \sigma = \sum_{k=1}^{\omega} (\rho_k - \sigma_k),$$

where the number of identities satisfied by the rows of D_k is $\rho_k - \sigma_k$, in view of 3.1. We can construct the following table, which, though it does not go very far, yields a convenient summary of our knowledge at the present time (**4**; **2**, p. 235).[2]

3.3

Weight	ρ_k	σ_k	$\rho_k - \sigma_k$
0	1	1	0
1	p	$p-1$	1
2	$\frac{1}{2}p(p+3)$	$\frac{1}{2}(p-1)(p+2)$	$p+1$

In what follows we shall be concerned, for the most part, with representations belonging to a fixed block of weight b, so we may drop the subscript k.

The problem of actually constructing the set of identities associated with B was solved by Chung (**2**, §3). He began with the fundamental character relation

3.4
$$\sum_{\alpha} \chi_\alpha(R)\chi_\alpha(S) = 0, \qquad \text{all } [\alpha],$$

which is to remain valid for any p-regular element of S of S_n. Thus R must be p-singular and we may set it equal to $P_k V$, where P_k is a cycle of length kp. Applying the Murnaghan-Nakayama recursion formula and the orthogonality relations for the characters of $S_n - kp$, we obtain

3.5
$$\sum_{\alpha} a_{\alpha\beta_k}\chi_\alpha(S) = 0 \qquad (k = 1, 2, \ldots, b),\ [\alpha] \subset B,$$

[2]Chung's determination of the *number* of ordinary and modular irreducible representations belonging to a p-block of weight 2 with zero core is applicable to the case of arbitrary p-core, in consequence of the theorems proved in this paper.

where $[\beta_k]$ is the residual diagram left after removing a kp-hook of parity $a_{\alpha\beta_k}$ from $[\alpha]$. Of course all $[\beta_k]$ have p-core $[\alpha_0]$, so *the summation in* 3.5 *may be limited to those* $[\alpha]$*'s belonging to* B. Writing

$$\chi_\alpha(S) = \sum_\lambda d_{\alpha\lambda}\phi_\lambda(S),$$

where $\phi_\lambda(S)$ is the character of S in the irreducible modular representation λ, Chung obtained the identities

$$3.6 \qquad \sum_\alpha a_{\alpha\beta_k} d_{\alpha\lambda} = 0 \qquad (k = 1, 2, \ldots, b), [\alpha] \subset \mathrm{B},$$

for all λ in B.

Conversely, let us assume the existence of a relation

$$3.7 \qquad \sum_\alpha a_\alpha d_{\alpha\lambda} = 0, \qquad [\alpha] \subset \mathrm{B}.$$

Retracing our steps, we conclude the existence of a relation

$$3.8 \qquad \sum_\alpha a_\alpha \chi_\alpha(S) = 0, \qquad [\alpha] \subset \mathrm{B},$$

for any p-regular element S of S_n. If we consider the columns of the character table as a mutually orthogonal set of vectors spannnig the space, then it follows that *any equation* 3.8 *must be linearly dependent on the set of equations* 3.4. But we have seen how these can be broken up into sets of equations 3.6 applicable to the separate blocks. Thus we have proved that

3.9. *Chung's system of identities satisfied by the rows of D is complete.*

4. Star ordering of Young diagrams. Let us denote the set of Young diagrams $[\alpha]$ belonging to B, or alternatively, the set of their representative star diagrams according to 2.4, by the symbol (b, α_0). If we remove a p-hook from each $[\alpha]$, i.e., a node from each of the representative star diagrams of (b, α_0), it is not difficult to see that the residual diagrams $[\beta_1]$ are just those of the set $(b-1, \alpha_0)$. Similarly, removing a $2p$-hook, where possible, from the $[\alpha]$'s yields the diagrams $[\beta_2]$ of the set $(b-2, \alpha_0)$. That we can identify the $[\beta_k]$ in this simple way follows from our Main Theorem. Proceeding in this manner we can write Chung's relation matrix in the form

$$4.1 \qquad A = (a_{\alpha\beta_k}) \begin{cases} [\alpha] \text{ ranging over the set } (b, \alpha_0), \\ [\beta] \text{ ranging over the set } (b-k, \alpha_0) \text{ with } k = 1, 2, \ldots, b. \end{cases}$$

The coefficients $a_{\alpha\beta_k}$ are ± 1 or zero according as the kp-hook removed is of even or odd leg length or does not exist, to yield the residual diagram $[\beta_k]$ of the set $(b-k, \alpha_0)$ at the head of the column in question. We shall denote the matrix consisting of rows (b, α_0) and columns $(b-k, \alpha_0)$ by $M(b-k, \alpha_0)$. The equations 3.6 may be summarized in the equation

$$4.2 \qquad A' D = 0,$$

where A' is the transpose of A.

Chung arranged the $[\alpha]$'s of (b, a_0) according to their *natural* or dictionary ordering. Largely for its intrinsic interest we define now a *star ordering* which will depend on the ordering of the associated star diagrams. For a diagram $[\beta]$ we may write

4.3 $$[\beta]_S^* = [\mu_0]\cdot[\mu_1]\cdot \ldots \cdot[\mu_{p-1}]$$

as in 2.2, where $[\mu_r]$ contains c_r nodes and

4.4 $$b = c_0 + c_1 + \ldots + c_{p-1}.$$

We shall say that $[\alpha]$ *precedes* $[\beta]$ *in the star order if:*

(i) $b_0 = c_0, b_1 = c_1, \ldots, b_r > c_r$;

or if

(ii) $b_r = c_r$ $(r = 0, 1, \ldots, p-1)$ *and*

$[\lambda_0] = [\mu_0], [\lambda_1] = [\mu_1], \ldots, [\lambda_s]$ *precedes* $[\mu_s]$ *in the natural order.*

As an illustration we shall rearrange the rows of Chung's table (**2**, p. 317) according to this ordering. The constituent of the star diagram preceding the vertical stroke is assumed to be of class 0, and that following it of class 1; here, of course, $p = 2$. This table illustrates also the application of our Main Theorem.

$[8]$ .... |	$[6, 2]$ ... |.	$[3^2, 2]$:|..	$[7, 1]$ |....
$[6, 1^2]$:** |	$[4, 2^2]$:* |.	$[2^4]$:|:	$[5, 1^2]$ |:**
$[4, 3, 1]$ :: |	$[2^3, 1^2]$:|.	$[5, 3]$.|...	$[3, 2^2, 1]$ |::
$[4, 1^4]$:* |	$[4^2]$ ..|..	$[3^2, 1^2]$.|:*	$[3, 1^5]$ |:*
$[2, 1^6]$:|	$[4, 2, 1^2]$ ..|:	$[2^2, 1^4]$.|:	$[1^8]$ |:

If, in addition to the rows, the columns of each set $(b - k, a_0)$ are rearranged in star order, then we shall denote the resulting matrix by A^*. Similarly we may star order the rows of D to obtain D^*. Of course these changes could have been made by using a transforming matrix, but it is clear that the relation $A^{*\prime} D^* = 0$ still holds.

5. The independence of Chung's identities. The proof of the following lemma follows immediately from the independence of the representations of the set $(b - k, a_0)$.

5.1. *The columns belonging to any set* $(b - k, a_0)$ *of* A, *that is, of* $M(b - k, a_0)$, *are linearly independent.*

While the columns of any given set are linearly independent, yet the columns belonging to different sets may very well be dependent, as Chung showed. The question arises: do Chung's relations between the columns of different sets exhaust the possibilities?

As referred to already, the character of any element R in $[\mathfrak{a}]$ can be obtained by considering the removal of successive hooks from $[\mathfrak{a}]$ which correspond to the cycles of R (**7**, p. 290). The $\pm$ 1's which appear in the row $[\mathfrak{a}]$ of A and lie in $M(b-k, \mathfrak{a}_0)$ pick out those representations of S_{n-kp} which contribute to $\chi_{\mathfrak{a}}(R)$. Thus for columns of $M(b-k_1, \mathfrak{a}_0)$ to be dependent on columns of $M(b-k_2, \mathfrak{a}_0)$, with $k_1 \neq k_2$, implies a relation of the form

$$5.2 \qquad \sum_i a_i \operatorname{col}_i M(b-k_1, \mathfrak{a}_0) = \sum_j b_j \operatorname{col}_j M(b-k_2, \mathfrak{a}_0).$$

To say that 5.2 is valid for all $[\mathfrak{a}]$ of B means that it is valid for those elements of the form $P_{k_1} P_{k_2} V$ which contribute to both sides of the equation. For such elements we can represent both sides of 5.2 in the form

$$5.3 \qquad \sum_z c_z \operatorname{col}_z M(b-k_1-k_2, \mathfrak{a}_0)^\circ$$

where

$$5.4 \qquad M(b-k_1-k_2, \mathfrak{a}_0)^\circ = M(b-k_1, \mathfrak{a}_0) M(\overline{b-k_1}-k_2, \mathfrak{a}_0)$$
$$= M(b-k_2, \mathfrak{a}_0) M(\overline{b-k_2}-k_1, \mathfrak{a}_0).$$

The expression 5.3 implies the restriction of the k's given by Chung (**2**, p. 220). Clearly the number of independent expressions 5.3 is just the number of irreducible representations of $S_{n-k_1p-k_2p}$ with p-core $[\mathfrak{a}_0]$, i.e., the number of members of the set $(b-k_1-k_2, \mathfrak{a}_0)$. Taking all possible k_1 and k_2 we obtain precisely Chung's relations between the identities.

5.5. *All linear relations between the columns of A are expressible in terms of the independent relations obtained by Chung.*

In §3 we denoted the number of representations belonging to a block B_i by ρ_i, and the number of indecomposables or modular irreducible representations belonging to B_i by σ_i. Thus the number of identities satisfied by the rows of D_i will be $\rho_i - \sigma_i$, and it follows from 5.1 and 5.5 that this number is equal to the number of Chung's identities which are linearly independent. According to Chung's procedure, this number $\rho_i - \sigma_i$ is a function of the following two determinations:

(a) The number of distinct sets $k_1, k_2, \ldots, k_r$ with $k_i \neq k_j$, $i \neq j$, and $k_i > 0$ for all i and j, and such that $\sum k_i \leqslant b$;

(b) The number of members of the sets $(b-k, \mathfrak{a}_0)$.

Now it is clear that the number of solutions of (a) depends only on n and b and not on $[\mathfrak{a}_0]$, and the number of members of $(b-k, \mathfrak{a}_0)$ in (b) is also independent of $[\mathfrak{a}_0]$ by our Main Theorem. Thus we have the following result:

5.6. *The number of indecomposables or modularly irreducible representations belonging to any p-block is independent of the p-core.*

The two results 2.6 and 5.6 provide a proof of Chung's conjecture.

References

1. R. Brauer and G. de B. Robinson, *On a conjecture by Nakayama*, Trans. Royal Soc. Canada, Sec. III, vol. 40 (1947), 11-25.
2. J. H. Chung, *On the modular representations of the symmetric group*, Can. J. Math., vol. 3 (1951), 309-327.
3. F. D. Murnaghan, *The characters of the symmetric group*, Proc. Nat. Acad. Sci., vol. 37 (1951), 55-58.
4. T. Nakayama, *On some modular properties of irreducible representations of a symmetric group* I, Jap. J. Math., vol. 17 (1941), 89-108.
5. ———, II, *ibid*, 411-423.
6. T. Nakayama and M. Osima, *Note on blocks of symmetric groups*, Nagoya Math. J., vol. 2 (1951), 111-117.
7. G. de B. Robinson, *On the representations of the symmetric group* III, Amer. J. Math., vol. 70 (1948), 277-294.
8. ———, *Induced representations and invariants*, Can. J. Math., vol. 2 (1950), 334-343.
9. ———, *On the modular representations of the symmetric group*, Proc. Nat. Acad. Sci., vol. 37 (1951), 694-696.
10. R. A. Staal, *Star diagrams and the symmetric group*, Can. J. Math., vol. 2 (1950), 79-92.
11. R. M. Thrall and G. de B. Robinson, *Supplement to a paper by G. de B. Robinson*, Amer. J. Math., vol. 73 (1951), 721-724 (cf. 7 above).

The University of Toronto

ON THE IRREDUCIBLE REPRESENTATIONS OF THE SYMMETRIC GROUP

MASARU OSIMA

Introduction. Let T be a Young diagram of n nodes:

$$T = [a_i]: \quad a_1 \geqslant a_2 \geqslant \ldots \geqslant a_h, \qquad \sum_{i=1}^{h} a_i = n, \tag{1}$$

a_i being the length of its ith row. With respect to a prime p, we denote by T_0 the p-core of T. If T_0 consists of m nodes, then

$$m = n - lp, \tag{2}$$

where l is the number of successive p-hooks [3] removable from T to yield its p-core T_0. We have stated in [4] the following theorem:

If T_0 is a p-core, diagrams T with T_0 as p-core are in one-to-one correspondence with systems $(D_1, D_2, \ldots, D_p)$ of p diagrams.

As an application of this theorem, in §1 the properties of self-associated diagrams will be studied. In §2 we shall give a recurrence formula for the number of irreducible representations and the number of self-associated irreducible representations of a symmetric group.

1. If the rows and columns of a diagram T are interchanged, we obtain another diagram. This is called the *associated diagram* of T, and is denoted by $\bar{T}$. If $T = \bar{T}$, then T is called the *self-associated diagram*.

Since a diagram T with T_0 as p-core is completely defined by a system $(D_1, D_2, \ldots, D_p)$ of p diagrams, we set

$$T = \{T_0; D_1, D_2, \ldots, D_p\}. \tag{3}$$

Let D_i contain l_i nodes; $l_i = 0$ when D_i is void. Then

$$l = \sum_{i=1}^{p} l_i. \tag{4}$$

From Robinson's fundamental theorem [5, p. 287; 4], we obtain readily

LEMMA 1. *Two diagrams $\{T_0; D_1, D_2, \ldots, D_p\}$ and $\{T'_0; D'_1, D'_2, \ldots, D'_p\}$ are associated if and only if $\bar{T}_0 = T'_0$ and $\bar{D}_i = D'_{p-i+1}$ for $i = 1, 2, \ldots, p$.*

Received November 20, 1951.

From Lemma 1 we have

THEOREM 1. *A diagram* $\{T_0; D_1, D_2, \ldots, D_p\}$ *is self-associated if and only if* T_0 *is self-associated and* $\bar{D}_i = D_{p-i+1}$ *for* $i = 1, 2, \ldots, p$.

We denote by $B(T_0)$ the p-block of the symmetric group S_n of degree n corresponding [1, 4] to the p-core T_0. If T_0 is self-associated, then $B(T_0)$ is called the *self-associated block* of S_n. From Theorem 1 we obtain

THEOREM 2. *Let* T_0 *be a* p*-core containing* m *nodes. The number of self-associated irreducible representations belonging to the self-associated block* $B(T_0)$ *of* S_n *is determined by* l *and is independent of* n *and* m.

We denote by $a(n)$ and $u(n)$ the number of diagrams and the number of self-associated diagrams containing n nodes. Then the number of irreducible representations and the number of self-associated irreducible representations of S_n are equal to $a(n)$ and $u(n)$ respectively. Denote by $v(n)$ the number of pairs of associated irreducible representations of S_n. Then

$$a(n) = u(n) + 2v(n). \tag{5}$$

Let $b(n)$ be the number of irreducible representations of the alternating group A_n. Then we have [2, p. 171]

$$b(n) = 2u(n) + v(n), \qquad n > 1. \tag{6}$$

2. We consider in this section the particular case when $p = 2$. Let $\{T_0; D_1, D_2\}$ be a diagram containing n nodes. Then we have from (2), $n = m + 2l$. We denote by $c(l)$ the number of irreducible representations belonging to the 2-block $B(T_0)$ of S_n. Then we see that

$$c(l) = \sum_{t=0}^{l} a(t)a(l-t). \tag{7}$$

LEMMA 2. *A diagram* $T = [a_i]$ *is a 2-core if and only if* $a_i = h - i + 1$ *for* $i = 1, 2, \ldots, h$.

Let $d(n)$ be the number of 2-cores containing n nodes. Then from Lemma 2,

$$d(n) = \begin{cases} 1 & n = \frac{1}{2}k(k+1) \\ 0 & n \neq \frac{1}{2}k(k+1) \end{cases} \qquad (k = 0, 1, 2, \ldots). \tag{8}$$

Further we have

$$a(n) = \sum_{l} d(n - 2l)c(l). \tag{9}$$

Hence (7), (8), and (9) yield the following

THEOREM 3. *For a given integer* n, *let* l_i $(i = 1, 2, \ldots, r)$ *be solutions of the equations* $n - 2l = \frac{1}{2}k(k+1)$ $(k = 0, 1, 2, \ldots)$ *in non-negative integers. Then*

$$a(n) = \sum_{i=1}^{r} \sum_{t=0}^{l_i} a(t)a(l_i - t),$$

where $a(n)$ *denotes the number of irreducible representations of* S_n.

n	$u(n)$	$v(n)$	$a(n)$	$b(n)$
2	0	1	2	1
3	1	1	3	3
4	1	2	5	4
5	1	3	7	5
6	1	5	11	7
7	1	7	15	9
8	2	10	22	14
9	2	14	30	18
10	2	20	42	24
11	2	27	56	31
12	3	37	77	43
13	3	49	101	55
14	3	66	135	72
15	4	86	176	94
16	5	113	231	123
17	5	146	297	156
18	5	190	385	200
19	6	242	490	254
20	7	310	627	324
21	8	392	792	408
22	8	497	1002	513
23	9	623	1255	641
24	11	782	1575	804
25	12	973	1958	997
26	12	1212	2436	1236
27	14	1498	3010	1526
28	16	1851	3718	1883
29	17	2274	4565	2308
30	18	2793	5604	2829
31	20	3411	6842	3451
32	23	4163	8349	4209
33	25	5059	10143	5109
34	26	6142	12310	6194
35	29	7427	14883	7485
36	33	8972	17977	9038
37	35	10801	21637	10871
38	37	12989	26015	13063
39	41	15572	31185	15654
40	46	18646	37338	18738

Example. For $n = 9$, we have $l_1 = 4$ and $l_2 = 3$. Hence

$$a(9) = \sum_{t=0}^{4} a(t)a(4-t) + \sum_{t=0}^{3} a(t)a(3-t)$$
$$= 20 + 10 = 30.$$

From Lemma 2 we have immediately

LEMMA 3. *A 2-core is self-associated.*

Let $\{T_0; D_1, D_2\}$ be a self-associated diagram containing n nodes. According to Theorem 1, we obtain $\bar{D}_1 = D_2$. If D_1 contains s nodes, then $l = 2s$ and $n = \frac{1}{2}k(k+1) + 4s$. Hence we obtain

THEOREM 4. *For a given integer n, let s_i $(i = 1, 2, \ldots, q)$ be solutions of the equations $n - 4s = \frac{1}{2}k(k+1)$ $(k = 0, 1, 2, \ldots)$ in non-negative integers. Then*

$$u(n) = \sum_{i=1}^{q} a(s_i)$$

where $u(n)$ denotes the number of self-associated representations of S_n.

Example. For $n = 21$, we have $s_1 = 5$ and $s_2 = 0$. Hence

$$u(21) = a(5) + a(0) = 7 + 1 = 8.$$

Now from (5) and (6) we can easily determine the number $b(n)$ of irreducible representations of the alternating group A_n. The accompanying table gives the values of $u(n)$, $v(n)$, $a(n)$, and $b(n)$ up to $n = 40$.

REFERENCES

1. R. Brauer and G. de B. Robinson, *On a conjecture by Nakayama*, Trans. Royal Soc. Canada, Sec. III, vol. 40 (1947), 11-25.
2. F. D. Murnaghan, *The theory of group representations* (Baltimore, 1938).
3. T. Nakayama, *On some properties of irreducible representations of a symmetric group* I, Jap. J. Math., vol. 17 (1941), 89-108.
4. T. Nakayama and M. Osima, *Note on blocks of symmetric groups*, Nagoya Math. J., vol. 2 (1951), 111-117.
5. G. de B. Robinson, *On the representations of the symmetric group* III, Amer. J. Math., vol. 70 (1948), 277-294.

Okayama University,
Japan